IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received February 22, 2022, accepted March 2, 2022, date of publication March 8, 2022, date of current version March 18, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3157850

Consent Receipts for a Usable and Auditable Web of Personal Data

VITOR JESUS[1] **AND HARSHVARDHAN J. PANDIT**[2]
[1]Aston Business School, Aston University, Birmingham B4 7ER, U.K.
[2]ADAPT Centre, Trinity College Dublin, Dublin 2, D02 PN40 Ireland

Corresponding author: Vitor Jesus (v.jesus@aston.ac.uk)

This work was supported by the European Union's Horizon 2020 Research and Innovation Program Next Generation Internet (NGI) Trust for Project 3.40 Privacy-as-Expected: Consent Gateway under Grant 825618. The work of Harshvardhan J. Pandit was supported in part by the Irish Research Council Government of Ireland Postdoctoral Fellowship under Grant GOIPD/2020/790, in part by the European Union's Horizon 2020 Research and Innovation Program NGI Trust for Privacy as Expected: Consent Gateway Project under Grant 825618, and in part by the ADAPT Science Foundation Ireland (SFI) Centre for Digital Media Technology funded by Science Foundation Ireland through the SFI Research Centre Program Co-Funded under the European Regional Development Fund (ERDF) under Grant 13/RC/2106_P2.

ABSTRACT Consenting on the Web, in the context of online privacy and data protection, is universally accepted as a difficult problem, mainly because of its cross-disciplinarity. For example, any approach to online Consenting needs to meet usability, legal, regulatory, technical, and business requirements. To date, effort has been predominantly focused on meeting compliance with regulations and automation, and less on the true re-empowerment of users with respect to their personal data. One approach that has not seen sufficient research is the use of '*Consent Receipts*', which offer a new paradigm of recording interactions concerning consent and using them as proofs in future actions, similar to familiar use of a common shopping receipt. In addition to being a record, receipts encourage accountability in how technology handles consent and is beneficial for all involved stakeholders. For organisations, it assists with legal requirements for demonstration of valid consent, while for users it provides transparency and accountability by being a proof to be used against malpractices related to consent. Receipts also have uses in addition to those related to consent, such as for authorising the holder in exercising related rights. This paper analyses the requirements, uses, and benefits offered by *Consent Receipts* with an extensive and broad literature review. Since receipts are a novel concept, we identify properties and requirements, and then new mechanisms necessary for the Web to support receipts. We then demonstrate feasibility of receipts through proof-of-concepts in three common real-world use-cases: (a) acceptance of a privacy policy and its subsequent changes; (b) choices expressed via consent dialogues or cookie banners; and (c) verbal interactions with Amazon Alexa.

INDEX TERMS Accountability, consent, GDPR, personal data, web, consent receipt.

I. INTRODUCTION

Consent and its management is a fundamental part of online privacy and data protection laws. A leading one, the European General Data Protection Regulation (GDPR) [1], defines requirements for '*valid*' and '*informed*' consent based on the provision of specific information to the user[1] and the manner in which choices and preferences are expressed. Providing information promotes transparency and encourages accountability by providing the ability to inspect conformance with legal requirements and (perceived) ethics. In addition, such laws also define the ability and mechanisms through which a choice made can be changed at a later time, e.g., to withdraw consent (GDPR Art. 7-3).

In practice, consent is approached as a legal compliance need rather than as a user empowerment and engagement tool. This is evident through the dysfunctional state of consent dialogues [2]–[4]. Even though it is increasingly apparent that consent practices on the web are largely non-compliant with the GDPR[2] [4]–[12], the notion of consent being a simple compliance problem that can be achieved through the single click of a button is distracting: it needs to change to

The associate editor coordinating the review of this manuscript and approving it for publication was Pedro R. M. InáCio.

[1]Though legal terminology, e.g. GDPR, has specific concepts associated with the roles and responsibilities of entities, such as Data Controllers and Data Subjects, we utilise the generic terms of Service Providers (or "Service") and Users for the sake of simplicity.

[2]See decision of the Belgian Data Protection Authority of Nov 2021: https://www.europarl.europa.eu/doceo/document/E-9-2021-005127_EN.html

something that is more user-centric and an enabler of benefits and accountability [13], [14].

For this, we argue that consent should be '*managed*' using first principles: that consent devolves into user empowerment and transparency, and the web acts an medium for expression of information and will.

Consent management has thus three key dimensions:

1) ensuring compliance with legal obligations;
2) user control of their personal data and consent actions over a period of time (rather than a one-off action); and
3) a user-centric, seamless, and usable process for actions.

Though laws, in principle, are codified to empower users, the ecosystem of consent practices is rife with malpractices. For example, the web is riddled with dark patterns[3] that subvert the individual's autonomy and puts in question the validity of given consent [5]–[8], [8], [10], [12]. In general, we see consent requests that are often malicious in their disregard of user choice [5]–[7] or practices that ignore privacy fundamentals and are designed for commercial interests [14]–[16], and implementations of dubious legality [5], [6], [12]. The net result is ubiquitous dialogues, banners, and virtually unreadable privacy notices seeking consent from the user in every form and interface they interact with, whether it be a website in a browser, a smart TV, or an app on their phone.

Where companies satisfy the need of providing information and seeking consent by providing a '*Consent*' (or, often, '*Agree*') button, the reality is that very few users exercise their will by actually analysing and reflecting on the given information [16]. Current privacy policies and notices are paradigmatic: they are dense with 'legalese' i.e. difficult to understand text which is antithetical to user expectations - and have thus rightly been called "*the biggest lie on the Internet*" [15]. Combined with the inevitable slowness of legal enforcement, this presents a challenge for achieving transparency and accountability. New mechanisms are therefore needed to ensure transparency and accountability on the web in a way that jointly benefits both services and users, and also assists regulators in supporting their investigations and enforcement actions.

Whereas abuse or malpractice of legal requirements is a problem, the *technical* counterpart is equally challenging: designing mechanisms and technologies for users to express and manage consent. The current paradigm of *Notice* (commonly mistermed as 'Privacy Policy') and consent encourages the practice of *consent once and forget*. A service provider collects consent following some (legal) requirements but leaves the user no recourse for later action or further information (e.g., how personal data is used or shared). This is because while the notice or consenting mechanism (e.g., a web popup), are available for changing the choices made at a later time - such as by visiting the website again and clicking some obscure button, the storage of choice itself is tied to the specific application or device – such as cookies stored within a web browser for that specific website. The non-ephemeral storage of consent choices is thus practically unavailable to the user and accessible only by the service provider (and in some cases shared with their partners).

As a result, consent on the web is the storage of consent choices which are accessible to a large number of companies and websites (via cookies or hidden mechanisms such as Real-Time-Bidding), which the user may or may not directly communicate with, and which is entirely obfuscated and hidden from the users themselves. As cookies may be deleted or overwritten, this results in no actual choice for users to modify or withdraw or even understand their consent choices. Similarly users have no knowledge of what consent choices have been signalled to other companies and how to access that information to change their decision at a later stage.

Therefore, in order to create an accountable balance between the user and the service provider, users should also receive and store a record of their choices. Ideally, users should be able to track how any and all of their personal data is being used regardless of what legal basis is used. However, we argue that *at least consent must result in actual user-empowerment* since it intended as a mechanism to do so, and that this requires more things than mere dialogue interactions.

Inspired by how we use shopping receipts, this paper is centred on *Consent Receipts*[4] - a digital artefact produced for recording interactions and particulars (what/who/where/why/how) regarding consent.

In practice, a Consent Receipt should be an extremely familiar scenario: upon consenting the user gets a *receipt* that can be used to: (i) demonstrate what their consent or what it is about; (ii) change their decision; (iii) request a change (up to deletion) about personal data; (iv) reuse information in other contexts such as a different consent interaction. This is similar to using a shopping receipt to provide proof of transaction and use it to return a product, request a refund, or claim tax-breaks. Thus, through consent receipts, users and companies not only get more options in managing consent and data, but also have opportunities for innovation in services based on reuse of information available through a receipt.

In this paper, we show that consent receipts can be designed to support many current requirements while being a familiar and easy to manage process. We first overview consent receipts with a focus on human and socio-technical factors regarding their usability and feasibility. Second, we elaborate on the properties of receipts considering the current state of online privacy and data protection and existence of relevant laws. Third, we demonstrate their practicality through three commonly experienced scenarios of website requests for consent (such as through forms), cookie and consent dialogues provided by third-party Consent Management Platforms (CMP), and for a screen-less device (Amazon Alexa) where the receipt has to be sent through other communication channels.

[3] See the recent (Jan'22) fine from the French regulator to Google (Deliberation SAN-2021-023) and Facebook/Meta (Deliberation SAN-2021-024) about illegal consent practices.

[4] Sometimes called Personal Data Receipts and similar variations.

In this, we advance the state of the art, as outlined in Section.III-C, by further providing a detailed analysis of requirements across disciplines and creating a concrete proposal for the socio-technical utilisation of consent receipts on the web. In addition to addressing the challenges identified in [17], we also demonstrate the relevance and applicability of legal and standardisation efforts (see Section.III) and its implications for consent and consent receipts. Finally, the three real-world applications of consent receipt validate their usefulness as - (1) a powerful tool for legal compliance as well as user empowerment; and (2) a technically and practically feasible solution for users and user-agents.

The rest of the paper is structured as follows. Section II presents a detailed notion of Consent Receipts and how a careful design can meet technical, legal and usability requirements. Section III presents the wider related work in online Consenting. Section IV outlines the required building blocks for implementing Consent receipts on the web. Section V presents and discusses our implementation of Consent Receipts for the three use-cases and their results. Finally, Section VI concludes with a discussion on the future of Consent Receipts.

II. CONSENT RECEIPTS

This section elaborates on the different perspectives for understanding the role of Consent Receipt: as a user-enabling artefact, its use in the the ecosystem of personal data, and potential benefits.

A. RECEIPT AS AN ARTEFACT

A Consent Receipt is an artefact recording the state and context of a '*transaction regarding consent*'. This is similar to a conventional shopping receipt that records the exchange of money for a service or a product. Traditionally provided using paper, receipts are now also provisioned electronically with possibilities of copies for both sellers and consumers. Because of its inherent simplicity and familiarity as a mechanism to the average user, a receipt can have the following immediate properties:

1) small, portable, and easily stored - which is necessary for implementing and using receipts by user-agents such as web browsers and smartphone devices;
2) self-sufficient by containing all required (meta)data concerning the transaction - allowing use in investigations and audits by authorities;
3) instantly generated with little preconditions or information outside of the transaction itself - which satisfies the requirements to record consent without requiring additional interactions such as the creation of an account;
4) acts as an actionable artefact, such as proving 'ownership' of consent in future interactions such as changing choices made or withdrawing it completely;
5) creation and provision of *self-service points* in which the receipt is used as a self-sufficient means of authentication to provide related services; and
6) can be anonymous in itself without losing its efficacy where it may not need any identifying attributes since a receipt can be implemented as *bearer token* and embed verifiability without sacrificing privacy.

It is intuitive to draw immediate parallels between use of receipts and the 'privacy paradox' where users (generally) value online privacy but will nevertheless use services that compromise their privacy. To reconcile this, one perspective is to consider the user as a stakeholder in the value-creation process based on their use of consent to provide data in return of services [14]. Here the opposing notions of consent as a transaction and as a mechanism for user to choose their privacy can be balanced by restating the argument to instead ask whether users are empowered to choose how they want to transact their privacy. This notion further makes the idea of Consent Receipts an intuitive one, and works to abolish the widely accepted practice of ''the user is the product''. Therefore receipts also apply here given that it records the interaction or transaction for all parties involved, and is usable as the canonical 'proof' to recall or reuse this information at a later date. More importantly, this goes beyond simply providing a record of consent by following the implications of rights the receipt-holder is empowered with.

1) RECEIPTS DECOUPLE IDENTITY FROM AUTHENTICATION

Receipts are an especially elegant solution for decoupling identity from authentication of the individual, and are useful where there is a lack of other means or available solutions require disproportionate measures. This is particularly important for situations where the interactions are ephemeral or short-lived, such as a casual website visitor where follow-up interactions for consent usually necessitate the creation of an account, and even then the account is only useful for the company rather than all the entities associated with consent (e.g. third parties).

A receipt, if designed as a secure bearer token [17], provides a straightforward solution for both the service provider and the user to communicate and interact in a truly anonymous, but verifiable and secure, fashion. It decouples the identification and authentication problems from reusing sensitive identity information (such as ID cards) and instead provides a solution scoped to the context whereby the parties involved can determine their own methods for identity and identification.

If the receipts are utilised as bearer tokens, service providers can make available control panels that require no accounts or additional efforts in proving the identity and ownership for personal data. Such *self-service points* consist of a location or process for using the receipts to some end, such as - requests for deletion or correction, conflict resolution, or tracing personal data as it is shared. This is an important benefit as it mitigates the ongoing common practice of presenting disproportional hurdles to the exercising of rights by demanding proof of identity via sensitive shared documents such as identity cards or passport which themselves result in additional legal obligations [18], [19]. In dissuading such

practices, not only are users better placed to interact regarding their own data and privacy, but also benefit from not being exposed to security and privacy risks arising from potential of data leakage and identity fraud [20].

B. RECEIPTS IN THE WIDER ECOSYSTEM

Privacy and Data Protection is an ecosystem that has three (simplified) key entities: the Users, the Service Providers and, to use a broad term - *Watchdogs* that consist of entities investigating consent-related practices, such as national or international regulatory authorities, privacy and consumer interest groups, and ad-hoc communities. Receipts have clear value and benefits to each of the three categories of entities as presented in the following subsections.

1) BENEFITS TO USERS AND SERVICE PROVIDERS

For *users*, receipts provide proof of consent and context, and thereby permit storing and analysing their own activities and data sharing practices, exercising communication and rights with service providers, and more importantly, provide evidence in challenging malpractices involving their data.

Receipts benefit *Service providers* in at least two ways. First, as a bearer token users can anonymously authenticate in the role of ''owner of personal data'', which lessens the compliance burden to hold additional personal information that can further lead to additional compliance tasks and potential for data breaches. GDPR, in particular, emphasises the principle of retaining and using minimal data for required purposes, and stresses not requiring additional data purely for the sake of provisioning rights where other alternatives are available [21], [22]. Second, receipts vastly simplify fulfilling legal obligations related to recording and demonstrating valid consent (GDPR Art.7) by providing the mechanism to create, store, and use an authoritative copy of a record of consent. Further, the use of semantics and metadata in a receipt provides an opportunity to utilise it as machine-readable information towards (semi-)automated enforcing of legal compliance [23]. That this approach leads to interoperability and creation of standards is evident from the existence of existing efforts leading towards the same (see Section.III-D).

2) INNOVATION AS SELF-SERVICE POINTS

Receipts, by containing information related to authentication of identity, can lead to better processes for rights management and interactions between service providers and users through self-service points where the users only need to provide a valid and verifiable receipt to a) identify themselves implicitly; and b) access services and processes associated with the information in the receipt. This can permit a wide range of automated and semi-automated interactions, not only for consent - such as its withdrawal, re-confirmation, or change of choices and preferences -, but also in other related areas such as data portability or access requests, and customer care. As we later show in our implementations in V, such automation opportunities are easily capitalised and with little user intervention.

3) BENEFITS FOR WATCHDOGS

As for Watchdogs, receipts provide a systematic and machine-readable mechanism to gather and inspect data regarding practices and compliance from both the service provider and the user. More importantly, it provides valuable evidence in resolving disputes. For example, Facebook recently claimed that users willingly chose the data collection and sharing practices on its platforms based on their use of prominent banners and consent dialogues. However, users claim they did agree to targeted advertisements but were not aware of the extent regarding being profiled and surveilled [24]. In another case, there was a dispute between a social network that was using post addresses to send letters on behalf of registered users.[5] These users say they never accepted, or were aware of, that use of their personal data (such as addresses). The social network insists consent was taken by displaying a prominent banner.

It is very difficult to settle such disputes without a thorough investigation of practices. Furthermore, such investigations are costly as they need time and manpower to identify, acquire, and analyse the forensic artefacts used *at the time of consenting*, and *for the user in question*. This is further complicated by the users have no information or mechanism to present their version of events, and as such the only option is implicitly trusting the service provider and their records.

A receipt has the potential of trivially resolving these matters if both parties are required to produce (verifiable) receipts. The expectation is that, in the vast majority of cases, it is only a matter of comparing and verifying what information was provided, where, and when. It is not too dissimilar to the case of a customer claiming they bought a certain item at a store and the store saying it was bought elsewhere. If not for complete verification of facts, such as how the request was presented or how the consent was expressed, receipts are still a helpful tool in identifying the direction for further investigation based on information within the receipt representing established pertinent facts.

4) ENCOURAGING ACCOUNTABILITY AND USER-EMPOWERMENT

We stress that consent receipts are inspired in the very familiar notion of shopping receipts. Nevertheless, given that consent receipts are a fairly new concept, they represent a learning curve for use by users in terms of understanding what they are, how to use them, and how it benefits them. However, the machine-readable nature of consent receipts represents a great potential for automation and tooling to support the user in reducing 'consent fatigue'; it would further help with empowerment against predatory malpractices, especially those surrounding cookie and consent dialogues on the web.

As we show in later sections, consent receipts open new possibilities regarding user empowerment tools, such as web

[5] https://blog.malwarebytes.com/privacy-2/2019/08/nextdoor-neighborhood-app-sends-letters-on-its-users-behalf/

browsers, where receipts can be automatically generated following a transaction such as acceptance in a cookie dialogue. In this, the role of the user can range between extremes: from a completely transparent and oblivious experience, to a user that frequently and in detail inspects each receipt (and they could be numerous). We anticipate that browsers will be able handle all relevant aspects of the process – for example, there would be a receipt wallet with rich visualisation functionalities and access to self-service points (as discussed later). A major difference receipts can potentially bring is a universal method for managing permissions granted to various sites on the web – e.g. where web browsers provides a dashboard of receipts and allows the user to understand their privacy practices better whilst allowing easier single-click withdrawals in self-service portals. This provides users with an important resource in that they now have a directly actionable resource they can use to revoke their consent or even challenge a claim with the service providers or authorities without length technical investigations.

Receipts also address the issue of fraudulent consent in important situations where there is sensitive personal data involved. It would further help when consent relates to exploitative practices such as tacit agreements for large-scale invasive surveillance on the web. By capturing such agreements within consent receipts, users would be explicitly asking 'proof' of what they have exactly agreed to. This would encourage service providers to uphold accountability and transparency, similar to the way asking for shopping receipts encourages good practice against purchase of goods. For cases where service providers actually need the information or invasive practices, consent receipts serve as a method for them to demonstrate the user has indeed agreed to their stated terms and that they have a copy they can later inspect or use to change their mind. For such important changes to occur, consent receipts require some form of data literacy or user education regarding how receipts would function and how users should use them.

III. RELATED WORK

In this section we review related work on the broader topics of consent, its management, and representation of related information within the context of online digital services.

A. LEGAL REQUIREMENTS

The current paradigm of information to be provided for 'informed' consent is based on requirements arising from law for the individual to be fully informed before giving consent. Such requirements do not directly specify the method or interface for information provision, but merely dictate the type of information to be provided. Current common practices include use of a privacy notice at the time of requesting consent, either as a link or a consent dialogue.

In the case of GDPR, the information to be specified regarding consent comes primarily from Article 13 for data directly collected from an individual, and Article 14 for data collected from other sources. This information includes identity of the service provider, the personal data to be collected and the purpose(s) of its processing, and the recipients of the data is shared with. This information is important for the accountability of the organisation and vital in investigations of legal compliance [6], [7]. It should be noted that the current practice is for services to freely, and at will, update the privacy notice, which complicates an investigation. Only by trusting the service records (the very ones in doubt and under investigation) can one know which privacy notice applied for a particular user at a particular moment in time. Receipts simplify this problem by explicitly requiring a link to the specific version of notice applicable at the time of consent interaction [17].

In addition, laws also dictate the validity of the consenting process, with the onus of demonstration being on the service provider (GDPR Art. 7-1). Consent records, being intrinsically linked to legal requirements (though not constrained by it), must therefore '*capture*' and represent information about both notice and process.

While this paper focuses particularly on the consent practices on websites, the argument and application of consent receipts is readily extensible to other avenues, such as IoT devices and smartphone apps. The only difference is between the UI/UX paradigms, such as those utilised within smartphones and apps as compared to websites, and the options available for consent receipts being limited given the amount of control permitted by the device and its OS makers (in particular Apple for iOS and Google for Android). Regardless, such practices are now under close scrutiny from authorities [25] including potential large fines.[6] Receipts, therefore, are not specific to a particular medium or a technology, but represent a record primarily from and for the human who is consenting in these situations.

B. MACHINE-READABLE REPRESENTATIONS

Receipts should be in a machine-readable form so to permit digital tools and agents (such as a web browser) to utilise and operate over it. There have been several approaches to represent information regarding consent as machine-readable metadata through semantic vocabularies and ontologies, along with visualisation techniques. We here summarise the key related work. See Kurteva et al [26] for an in-depth survey on the use of semantics to represent various aspects and processes related to consent and consent management.

The EU funded SPECIAL H2020 project[7] developed ontologies to represent consent as a 'policy' [27] consisting of personal data, purpose, processing, recipients, and storage durations, to be stored on a distributed ledger for transparency and accountability. Information is wrapped in a semantic reasoner for facilitate compliance checking. Other projects and approaches that also define a similar semantic

[6]https://www.computerweekly.com/news/252495431/Grindr-complaint-results-in-96m-GDPR-fine

[7]https://specialprivacy.ercim.eu/

model of consent include MIREL[8] project's PrOnto ontology providing conceptual taxonomies [28], BPR4GDPR[9] project's compliance ontology based on process mining [29], RestAssured's[10] privacy model based on user preferences [30], and TRAPEZE[11] which extends SPECIAL project's work on consent towards managing user policies [31]. While their models suffice the requirement for a service provider to check its own consent 'validity' in an operational sense, the fields they represent is not sufficient to represent necessary information and context as required for the creation of a consent receipt.

Efforts modelling additional information associated with consent include GConsent[12] [32] semantic ontology which (also) bases its model on GDPR compliance. It is similar to the above efforts while additionally modelling attributes such as the method and medium of consent, as well as its 'state' indicating a 'lifecycle' of consent - as an artefact which starts when it is requested and ends when it is withdrawn or otherwise terminated.

The Data Privacy Vocabulary[13] (DPV) [33] is the outcome the W3C Data Privacy Vocabulary and Controls Community Group[14] (DPVCG) and represents a broad consensus amongst experts from the domains of data protection, privacy, legal compliance, and semantic web. DPV provides a semantic vocabulary consisting of hierarchical top-down taxonomies for specifying purposes, processing categories, personal data categories, technical and organisational measures. For consent, it presents concepts representing notice, expiry, provision, withdrawal, and whether the consent is explicit.

It is clear that the representation of consent as machine-readable information, especially through use of semantics, has seen both interest and progress. However, for the receipt to be used as we envision, data must use an interoperable format, necessarily needing a standard (e.g. RDF or JSON) and standardised vocabularies - such as from W3C DPVCG. In this, the challenge is to create vocabularies which are sufficient to represent the necessary information within different jurisdictions, while also providing a way to expand and specialise them for use-cases and specific domains as necessary.

C. USE OF CONSENT RECEIPTS

Consent Receipts as a conceptual framework where information regarding consent is documented and packaged already exist as identified in the following instances from the last 5 years. A report by Digital Catapult [34], in collaboration with the UK's Research and Innovation program, outlines the use of 'personal data receipts' for capturing information and increasing transparency and user trust. Several Consent Management Platforms (CMP), such as ConsentEye[15] and Signatu,[16] which act as the technology providers (i.e. Data Processors) for service providers to assist with requesting and managing consent through the use of dialogues and interfaces, also support the use of consent receipts in their frameworks. Additionally, a patent by OneTrust LLC regarding consent receipt management systems is of tangential relevance here [35].

While the above instances utilise receipts, they do so in an ad-hoc fashion where the receipts contain schemas defined by the company generating them without any recourse for proof and verification. For receipts to be verifiable and interoperable, the information requires cryptographic assurances to be provided by the parties that can be used to prove consent and elicit non-repudiation along with fair-exchange protocols to demonstrate a cryptographic receipt of acceptance [17]. In addition, receipts held only by the service provider are of marginal value. For receipts to be truly functional, there has to be parity in how they are used by the user proactively without relying on the service provider, which necessitates users to have access to their own copy of a receipt.

D. STANDARDS FOR CONSENT

The consent receipt is an '*end-of-process*' artefact as it is generated after some process or information regarding 'consent' has already taken place or is disseminated. Given that 'consent' has seen several standardisation efforts at various levels in the past and is the topic of ongoing efforts to produce agreement, this section summarises the most pertinent ones along with their implications on the design and utilisation of consent receipts.

The current specification for Consent Receipt by Kantara Initiative [36] offers an introduction to the concept, and is only a starting point towards an usable and practical receipt structure. The information fields specified by this iteration of the specification lack the necessary information required by recent changes in consenting mechanisms, such as the inclusion of GDPR requirements, or the necessity of ensuring receipts are verifiable.

To address these concerns, two new Working Groups[17] are underway. One is the Advanced Notice & Consent Receipt Working Group[18] (ANCR-WG); another is the CRWeb Project (Consent Receipts for the Web)[19] which is a directed effort to bring Receipts to dynamic web scenarios and able to cope with a range of requirements from static websites to dynamic browser signalling for privacy preferences (discussed in Section III-E).

[8] https://mirelproject.eu/
[9] https://www.bpr4gdpr.eu/
[10] https://restassuredh2020.eu/
[11] https://trapeze-project.eu/
[12] https://w3id.org/GConsent
[13] https://w3.org/ns/dpv
[14] https://www.w3.org/community/dpvcg/
[15] https://docs.consenteye.com/user-guide/consent-receipt
[16] https://edps.europa.eu/sites/edp/files/publication/16-09-09_documenting_consent_en.pdf
[17] Vitor Jesus is chair on both groups.
[18] https://kantarainitiative.org/confluence/pages/viewpage.action?pageId=140804260
[19] https://kantarainitiative.org/confluence/display/WGISI/CRWeb%3A+Consent+Receipts+for+the+Web.

Perhaps the most impacting specification is the Interactive Advertising Bureau's (IAB) Transparency Control Framework (TCF) which is behind the vast majority of ''cookie banner'', the latest being version 2.[20] TCF is a pseudo-standard or a soft-standard, given that it is a specification developed by IAB without any formal standardisation process and implemented under agreement by advertising industry companies and utilised in consent implementations by CMPs. It provides a structure for representing consent information for pre-defined data categories, recipients, and purposes. We use this framework, with software extensions to their APIs, in one of our use-cases (see Section.V-B). One should remark that, at the time of writing and as previously said, the TCF framework has been found to be in breach of the GDPR's requirements in a draft decision by the Belgian Data Protection Authority (see footnote.2) - which may bring dramatic changes to consenting mechanisms in the near future.

Of high relevance to this paper, the International Organization for Standardization (ISO) has produced the ISO/IEC 29184:2020[21] [37] standard for online privacy notices and consent, published recently in 2020. Of note is that while 29814 dictates the requirements for notices and requests for consent in terms of information provision, methods, and processes therein, it also specifically mentions machine-readable records of consent and cites the Consent Receipt [36] as an example of such a record. A comparison of 29184 and GDPR [38] requirements in terms of privacy notices and consent validity and practices demonstrates that they are largely compatible in terms of implementations. However, they differ in terms of conditions for validity of consent (e.g. explicit consent under GDPR has stricter requirements). This has implications on receipts generated under ISO/IEC specifications in term of how they should be interpreted towards legal compliance with laws such as the GDPR.

The finalisation and publication of 29184 in 2020 was followed by a currently ongoing effort at standardising the technical specification ISO/IEC 27560[22] for consent record information structure. This is, technically. a Consent Receipt albeit in a format (expected) to be simpler than what we here advocate given the lengthy and consensus-based process at ISO. It is expected to provide a standardised agreement on what information should be contained within a record of consent and its provision as a consent receipt. Work is still in early stages[23] but it is expected to produce a stable document by 2023.

Other notable efforts at standardising consent include domain specific activities regarding health data. The Fast Healthcare Interoperability Resources (FHIR) series of standardised specifications for exchanging electronic health records (EHR) was developed by the Health Level Seven International (HL7) non-profit. It contain components for expressing the consent[24] outlining the specifics of data and its use [39] within hospital, clinical, medicinal, and other health-data specific settings. As such, it is an interoperable record of consent within the health data or medical domain with a high-degree of awareness amongst domain experts and has seen successful uptake.

Similar to this effort, the Data Use Ontology[25] (DUO) is a vocabulary outlining the permissions/restrictions regarding data based on consent in the health and medical domains. It has been approved for use as a standardised vocabulary[26] by the Global Alliance for Genomics & Health (GA4HH).

E. PRIVACY PREFERENCE SIGNALLING

A 'Privacy Signal' or a 'Privacy Preference Signal' is a digital signal to be interpreted as indicating a preference regarding the data usage and sharing preferences of an user. Consent receipts may be generated as an explicit representations and proof of the choices conveyed through a privacy signal.

A recent survey paper outlines the history and salient features of web-based privacy signals with commentary on the political and economical challenges in achieving conformance and agreement over such signals. It shows that the trend is towards laws explicitly codifying requirements to respect such signals, with CCPA [40] being an example of an enforceable law explicitly suggesting use of a privacy signal; the proposed ePrivacy regulation [41] by the EU also containing clauses regarding the actionability of privacy signals.

1) DNT AND P3P)

The ''Do Not Track''[27] (DNT) is such a signal sent via HTTP headers to indicate the user's preference regarding tracking, and includes mechanisms for sites to communicate whether and how they honour a received preference and for tracking its status. DNT was largely panned by service providers due to not being an explicit preference by the user, with controversy over what the term 'track' was to be interpreted as, and whether software, such as web browsers, should be permitted to set it by default. As a result of these, the signal has largely been relegated to being not supported by companies as well as not considered actionable by law[28]

Other non-successful efforts involving privacy preferences and consent include the Platform for Privacy Preferences Project[29] (P3P) which specified a protocol allowing websites to declare how they use information they collect about web browser users and to match this with an user's preferences as a way of enabling users to exercise control. Developed and standardised by the W3C over a number of years,

[20] https://iabeurope.eu/tcf-2-0/

[21] https://www.iso.org/standard/70331.html

[22] https://www.iso.org/standard/80392.html. Both authors are members of the technical committee.

[23] As of January 2022, Working Draft 4 was under review.

[24] https://www.hl7.org/fhir/consent.html

[25] https://github.com/EBISPOT/DUO

[26] https://www.ga4gh.org/news/data-use-ontology-approved-as-a-ga4gh-technical-standard/

[27] https://www.w3.org/TR/tracking-dnt/

[28] Based on the fact that there have been no complaints or actions by authorities involving DNT, and nor has it been mentioned or acknowledged by any of their guidelines.

[29] https://www.w3.org/TR/P3P11/

P3P was eventually declared obsolete following non-adoption by service providers, criticisms of it being difficult to use and burdening users, and difficult in enforcement. Efforts at Internet Engineering Task Force (IETF) to develop mechanisms related to consent, such as RFC 5361,[30] were also not successful.

2) GPC AND ADPC

More recently, the Global Privacy Control[31] (GPC) is a similar (albeit potentially legally enforceable) signal based on the California Consumer Protection Act's [40] (CCPA) do-not-sell obligation which requires companies to not sell or share personal data with third-parties. The GPC is a boolean signal, similar to DNT in application, and has been authored and supported by several notable service providers, including the web browser Firefox.

The Advanced Data Protection Signal[32] (ADPC) is another privacy signal which specifies a mechanism by which the expression of choices regarding consenting to specific purposes or its withdrawal or exercising right to object can be automated using HTTP headers.

3) SIGNALS ON iOS AND ANDROID

Apart from web browsers, smartphone and device makers, most prominent Apple and Google, have also expressed their intention to develop such signals within their respective ecosystems. While Google is yet to present its planned solution, Apple has made recent changes to its App Store which requires apps and their developers to specify information about data collected and its use which is then displayed in a 'privacy label' on that app's page within the App Store. Apple has also mandated asking consent for tracking and profiling users[33] through its 'App Tracking Transparency' framework which prohibits the retrieval of device identifiers necessary to track advertising engagement within apps and on device until the user has given their consent.

IV. BUILDING BLOCKS OF RECEIPTS FOR THE WEB

One of the more promising aspects of Consent Receipts is that they can be bootstrapped readily, in a simpler format, without requiring any major changes to the current consenting practices. A minimal implementation of a receipt could be as simple as generating and sending it to the user using existing communication mechanisms such as through apps, a browser extension or email. However, to fully realise the vision of an accountable, transparent, and user-empowered Web, additional developments are needed to implement the necessary processes associated with utilisation of receipts and self-service points. These include architectural and implementation modifications within the consent interfaces to support receipts, semantic markup of content to annotate it for detection and utilisation by user-agents to generate receipts, and standardising to support interoperability between entities acting on the receipt.

A. STRUCTURE OF RECEIPTS

A key aspect is what information should be included in the receipt. Its structure and data should stem from the following considerations:

- understanding what consenting is about e.g. which categories of personal data;
- jurisdictional laws and regulations which mandate provision of information for 'informed consent' and define conditions for 'valid consent'; and
- contextual information whose existence provides benefits to a stakeholder - such as additional information on how to exercise their rights.

In this article, we focus on the first two categories of information given their necessity to realise receipts. The third category requires specific information and processes for concepts (e.g. for exercising rights). These are dependent on the jurisdiction which provides that right and the technological basis for exercising it. For these, we discuss how receipts can assist in providing information about such concepts and accessing them without requiring additional accounts or identifying information.

From the above, we broadly categorise information to be included within the consent receipt as follows.

1) GLOBALLY UNIQUE IDENTIFIER OF THE RECEIPT

If one wishes to make the receipt have bearer token properties, receipts should have a global identifier that should not be tied to any central point. Generating such identifiers locally is nowadays common practice with high likelihood of uniqueness e.g. as universally unique identifier[34] (UUID). Here the term *global* can be replaced with a similar concept that refers to the uniqueness of an identifier within a given context - such as specific to a service, company, or even for an individual. UUID-3 and UUID-5 both provide a way to generate namespace-based identifiers, whereas UUID-4 The primary requirement it represents is that the receipt should be uniquely identifiable (by all involved parties) within that context.

Even though the prevalence of mechanisms such as UUID may be sufficient to generate unique IDs, certain areas of application, such as where sensitive information is involved or which has potential for detrimental impacts on individuals, may require guarantees that the identifiers generated are collision-free. Such sensitive areas may choose to develop their own identification mechanisms.

2) PERSONAL DATA, ITS PROCESSING, AND PURPOSES

The receipt should contain the (types or categories of) personal data involved and the purposes it will be collected, used, stored, shared, and otherwise processed for, including the source, duration, and location of personal data and its relevant

[30] https://datatracker.ietf.org/doc/rfc5361/
[31] https://globalprivacycontrol.org/
[32] https://www.dataprotectioncontrol.org/
[33] urlhttps://developer.apple.com/app-store/app-privacy-details/
[34] https://datatracker.ietf.org/doc/html/rfc4122

processing activities. Where such personal data is considered to be of a sensitive or a special nature, this could be reflected in the receipt so as to indicate a higher requirement for privacy and data protection.

In addition, laws such as the GDPR specify provision of additional information in the context consenting, such as when technologies include automation or specific processes such as profiling - as part of the informed consent process. This information must similarly be included in the receipt. The consent receipt should not contain actual (instances of) personal data to avoid the receipt itself becoming an avenue for data misuse and risk, unless doing so is necessary.

3) IDENTITY OF RESPONSIBLE ENTITIES I.e. DATA CONTROLLERS

Depending on jurisdictional terminology and requirements, the entities responsible for carrying out the specified processing of personal data are required to be identified in the receipt. This is not always straightforward as the distinction between responsibility of a process and carrying it out might be interpreted as being distinct.[35] Ultimately though, the identity of an entity refers to a legal entity that must be specified for accountability purposes. Here we do not distinguish between controller, processor, joint controller, or other such terms given that they are entirely defined within respective jurisdictional laws, and that the commonality of such terms is the indication of *prima facie* the responsible entities. Typically, a 'processor' is not specified within this list given its reliance on being contracted by a controller, and that, if needed, processors can be declared under a separate category of recipients.

4) IDENTITY OF THE USER

A consent must be associated with an individual (a ''natural person'' as in GDPR) – also referred to as a user within the context of a service or as a Data Subject or PII Principal within legal/formal terms. Therefore the receipt must embed some notion of identification (and not quite *identity*) through which the information can be attributed to the individual and ownership can be established. Typically, this could be a known identifier, such as email address or specific accounts, or an ad-hoc, unique, perhaps secure, identifier created specifically to refer to the individual by the receipt-issuing entity, such as an internal identifier assigned to the individual. In our vision, we see *possession* of a receipt, if secure, as sufficient means for proof-of-ownership of the personal data and, hence, entitled to act on it – such as request deletion or correction.

While having an identifiable field could benefit authentication and verification processes in some cases, for privacy and security reasons it is ideal if no personal data of the data subject is part of the receipt. This is especially important for identifiers that are shared across other processes and which may lead to detrimental impacts to the individual in the form of data leaks or to the controller in the form of legal obligations and data breaches.

5) CONTEXT OF NOTICE AND CHOICE OF CONSENT

A receipt must capture the consent interaction which includes the surrounding information and processes. Typically, this involves the provision of some information in the form of a notice, which then also acts as the request for consent (e.g. a consent dialogue on a website using HTML/JavaScript). While the 'consent' information may only be limited to the fields related to personal data, purposes, entities, and so on, the context of *consenting* also involves the environments within which that interaction took place and the artefacts involved therein [17]. For example, it is straightforward to mislead the user into accepting terms by carefully using malicious JavaScript and hidden HTML controls.

Therefore, where possible and feasible, a receipt should include information or links to the privacy notice and the methods by which consent was requested or obtained or otherwise interacted with. This constitutes the 'context' of a consent interaction, and is important when determining the validity of consenting mechanisms and given consent for specific requirements within a privacy law. For example, the requirements for consent to be freely given under GDPR are inherently tied to the context in which that consent is interacted with.

Similarly, the context is also important in the sense that the current practices for how a notice is displayed and what choices it offers is rife with dark patterns which are manipulative and invalidate the given consent. While a receipt may not feasibly capture the entire environment, it can retain information such as a link to the notice and request being shown for later audits, a concept ISO/IEC 29184 reinforces.

6) JURISDICTION AND JURISDICTIONAL INFORMATION

The information to be represented within a receipt is heavily influenced by the jurisdictional laws. Therefore to ensure accurate interpretation of a receipt, the jurisdictions applicable for that particular interaction might need to be represented alongside this information. Examples of such information can simply denote a region, such as 'EU' or to specific laws such as 'GDPR'.

The '*applicability*' of jurisdictions is a complex topic based on the identities of entities involved, their geo-locations of operations, political concepts such as citizenship, and the scope of authorities as dictated by their governing laws. In practice, and particularly in dynamic web environments, it may not be possible to authoritatively assert the applicable jurisdiction. Instead, the service provider or controller can provide an acknowledgement of the jurisdictional laws it adheres to, such as by stating that since the user is within the EU they are governed by the GDPR.

[35]For example, in GDPR, the 'Controller' is defined as the entity that determines the processing of personal data, which could result in an entity that has no access to personal data being declared as its Controller if it has sufficient control of the means through which it is processed. Therefore, merely mentioning which entities have access to the data may not be sufficient to determine responsibility and accountability.

In addition to the above, jurisdictional laws may require the provision of additional and specific information related to the applicability of other features such as rights or complaint procedures. The receipt, given that it already specifies jurisdictional information, can also additionally be used to provide such information to the user for ease of access and to fulfil notice and information provision obligations.

7) THIRD-PARTIES AND DATA RECIPIENTS

A major issue with the current practices surrounding consent is the transparency and accountability related to data being shared, sold, or transferred to third parties under the guise of consent [6], [9], [42]. Even where a notice or dialogue specifies a list of such third parties, this information is often too dense and unclear as to who they are and what they do with the consented data [5], [6].

The receipt, being a provisioned digital record, can provide a complete and useful list of such entities along with relevant information such as their identities in the form of a specific legal identity, their role within the consent interaction, their policies, jurisdictions, contact information, and so on. Here we note that there is an independent relationship between the third party and the user in terms of the the consent choice or how that consent can withdrawn only for that particular third party. Therefore it is preferable for accountability and record-keeping purposes if each third-party also provided its own receipt back to the user.

8) LIFECYCLE MANAGEMENT

Because it is expected that the relationship between the user and service changes over time, as governed by the interactions regarding consent (e.g. request, give or refuse, withdraw), the receipt should indicate the current state of consent. For example, a request to withdraw a given consent can be exercised at any moment which requires establishing the previous context and/or a way to reference it. Receipts can do this. In return, the new interaction regarding withdrawal or revocation can itself lead to producing new receipts which reference earlier receipts for provenance and linking of information. In this sense, receipts can become the central element of a transactional protocol that lives across time, just like TCP/IP is for a network session.

Implementation of the notion of lifecycle can also permit users to track how their consent was initiated and used, and what options and limitations exist or apply over it. For example, a consent can have an expiry timestamp during which it is 'valid', unless terminated or revoked). This permits both service providers and users to periodically review their permissions and manage consent processes accordingly - such as to 'refresh' (often a requirement of GDPR) or 're-affirm' consent based on time or events associated with the lifecycle.

In addition, there may be a need to represent states which are typically not provided or acknowledged through the use of receipts, such as when consent is refused to be provided. In this case, the use of states and depicting it within a lifecycle offers several advantages, especially for users, to demonstrate that a particular interaction resulted in the prohibition of personal data collection and usage rather than a permission as could be assumed or claimed by the service provider. It also assists in cases where a user is requested to or wants to change their initial decision.

9) AUDITABILITY AND VERIFIABILITY

The receipts are intended to be an authoritative artefact to establish consent and as such to be a useful and actionable documentation of interactions. Therefore, they must be protected for non-repudiation, auditability, and should be verifiable by design. This points to needing use of cryptographic schemes and secure network protocols when creating the receipts. Greatly simplified, the core of the threat model for the use of receipts is an involved entity or party denying ever having issued the receipt or dispute its particulars. Thus, receipts face two challenges: (a) how to verify the receipt is associated with the entities involved; and (b) how to ensure the receipt is authentic and both copies (user and service) match and were the agreed on at the time of consenting. Jesus [17] offers an in-depth technical discussion and technical approach on this topic.

10) SELF-SERVICE POINTS

We argue that, for the sake of transparency, auditability and usability, receipts should come with (what we call) *self-service points*. This means receipts are generated with information about an endpoint (such as a URL/URI) for accessing features or services related to Personal Data, either relevant or additional to the receipt. All pertinent information necessary to access and interact with it in a self-sufficient capacity could be available using just the receipt. Examples of information relevant to self-service points could be the what is already present in a receipt, such as signatures, or additional information added specifically for the purposes of utilising such services, such as identifiers.

In practice, we envision such self-service points, similar to control panels, to be simple webpages that, on uploading the receipt, the user has access to personal data, can inspect any operations on it (including sharing) and make requests. Furthermore, and apart from convenience, self-service points can enable new ways to manage personal data (e.g. through agents) and enable exercising of rights and features without the need for additional, often sensitive, information for identity verification, which is a barrier to their effective utilisation today [18], [22], [43].

B. ARCHITECTURE OF A WEB WITH RECEIPTS

In order to support consent receipts, the web and internet-based applications (e.g. mobile apps) need to support the essential mechanisms associated with receipt generation, utilisation, and verification. Figure 1 illustrates a simplified architectural overview of the different components, functionalities, and relationships involved in utilising consent receipts on a personal device. Through this simplification, we hope

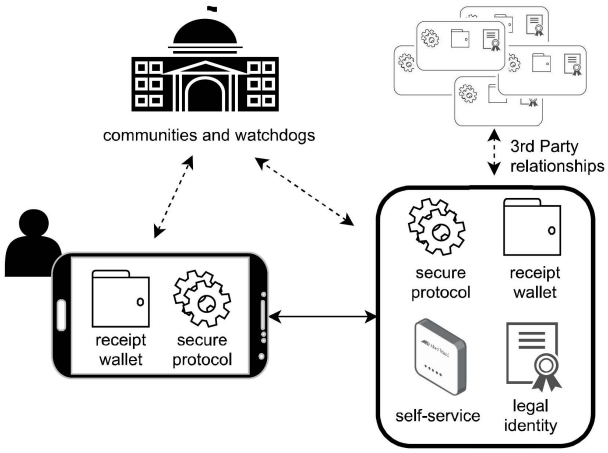

FIGURE 1. Architecture of a Web with Consent Receipts.

to illustrate the applicability towards the wider web-based privacy and data protection landscape.

The diagram shows four key entities. The first one, central to this paper, is the user and their (personal) device. Second is the online service (provider) that collects personal information from the user and holds responsibility for its usage and processing. Other than these two, the figure also shows the other two key stakeholders representing third parties and watchdogs. The third parties, who might be each a service provider on their own, obtain personal data from the (primary) service provider either directly (i.e. data is shared or transmitted by the service provider) or indirectly (i.e. enabled by service provider to obtain data from the user). The second category of stakeholders represents the wider community of watchdogs who have an interest in the investigation of practices, and consist of entities typically acting as regulators, authorities, consumer protection organisations, and NGOs.

On the user side, the user-agent or application used to support consent receipts needs two new components. First, it needs a special storage mechanism to collect, store and manage receipts. We anticipate that, should consent receipts become common, a single user could collect many receipts per day based on their interactions through the web. Therefore, for efficiency and friction-less usage, the storage mechanism needs implementation of a supported component within the environment which enables interactions with other entities necessitating a receipt. Typically, this would be web browsers for websites and the smartphone's operating system for its applications. In our implementation (see Section V), we targeted a web browser through development of an extension that collects receipts and stores them in a searchable database.

The second component on the user side is a secure transactional protocol. As discussed before, a receipt will be of little use if one cannot trust its contents. All entities or parties need to validate and commit to the contents in the receipt. For example, the underlying privacy notice needs to be signed by both to represent its provision and acknowledgement, For this a digest of their signatures could be stored within the receipt. We point to existing external work that discusses and demonstrates its implementation and feasibility [17], [44].

On the service provider side, a similar component must exist in order to run the secure protocol that can sign and verify receipts. Given that the service provider may be dealing with a lot of receipts, this necessitates a solution that can function potentially at scale. Therefore, the 'wallet' used to store and retrieve receipts may be functionally different for service providers from that of the users depending on integration with existing technologies and frameworks used. It is important to note that even where a service provider may decide to store information in a different form from that contained within a receipt, the intention of the receipt is to be able to act as an verifiable claim between the service provider and the user. Therefore as long as the service provider can produce the receipt from its stored information, and can match and verify it against a receipt claimed by the user, this is sufficient for the intended functioning of receipts.

In terms of identities, the users should not need to present an official identity (e.g., passport) state-accredited form of identity to produce a receipt; the service provider, however, must provide some form of identity, even if a SSL certificate or ownership of a domain name.

Finally, as illustrated in the figure, and not necessarily a required component but rather a feature of consent receipts, we envision that service providers will offer a ''self-service point'' as discussed previously. Using the receipts, and strictly not needing anything else, users could independently manage their personal data to the extent to the law (e.g., withdraw consent or request data deletion) or the extent the service provider is capable or comfortable with.

C. EXTENSIONS TO THE WEB

Supporting receipts involves information associated with the service provider's practices, which currently is provided to the user via notices or consent dialogues. There is a glaring lack of ways for specifying such information at two important levels: first, the HTML - e.g. tags for indicating notice or policy; and second, the semantic level - e.g. schema.org[36] tags to specify the contents within a notice, consent request, or a privacy policy. The use of automated signals, such as DNT and GPC, are sufficient, in some cases, to indicate choice but are weak by themselves for use as evidence without some form of 'record' indicating they were applied by the user, and conformed to by the service provider.

While this paper and section substantially focuses on the web as in websites, it is important to note that the approach and argument applies equally to personal devices. Such devices, in particular smartphones, are platforms significantly controlled by manufacturers. Restriction and features related to data collection through use of APIs typically lack the means to request and record consent, even more so in a human-friendly way. Apple's recent efforts in providing clear privacy-oriented labels in their App Store, and the

[36]https://schema.org/

requirement for consent, seem to be an effective push in this direction [45], though it still faces the issue that there is no way to track where, when, and for what was consent given.[37]

In order to implement receipts, collective changes are required across the web and app platforms, ideally by way of standards development and their adoption. Given the widespread prevalence of consent interactions on the web, it is rather surprising to not have any mechanisms through which it can be made easier for end-users to interact with or for service providers to request and manage information. In the following paragraphs, we outline directions for implementations and their practicality in terms of development and adoption for improving the web ecosystem towards better information and consent practices.

1) DECLARATIVE INFORMATION ON WEBPAGES

HTML is effectively a machine-readable language through which the web browser (as an user agent) can graphically display information and means for interaction. Aligned efforts, such as schema.org, provide the means to embed additional contextual semantic information so as to assist machine-agents (such as search engines) with understanding the content on a web page and enabling smarter features such as recommendations and summaries. This mechanism for annotating webpages can be extended (as described in Section IV) to describe information and processes associated with consent – e.g., privacy notices, terms & conditions, or identities of service providers. While it is a challenge to represent this information in a jurisdiction-agnostic way, and to keep the web as open and global as possible, the existence of ISO/IEC standards and their use of common vocabularies as representative of global agreement on terminology demonstrates the possibility and feasibility of such as an approach.

The placement of annotations within a webpage could be at a global level, by using the HTML `<meta>`) tags so as to indicate its applicability to the entire website or domain, or declared locally within a particular HTML element (e.g. `<section>` to indicate separation from other matters. Through this, a consent dialogue can contain machine-readable annotations to accompany the human-readable text, and also enable automation in their interactions regarding consent.

The machine-readable information declared in this way can be easily parsed and interpreted by user-agents such as the browser and utilised in mechanisms such as generating the receipt or using accessibility features. In addition, it can also help mitigate manipulative practices of dark patterns by generating a notice entirely at the user-side, or to incorporate user preferences in the design. To enable such developments, it is critical for the web to develop dedicated elements to depict and handle 'notice' and 'consent' as first-class processes on the web.

Additionally, annotations provided on a webpage also permit declaring existence and support for receipt-aligned protocols and services such as use of 'wallet' and 'self-service' endpoints that can also utilise the machine-readable information. This can permit further feature-rich interactions by having user-agents assist users in finding required information, such as where to access a privacy policy or contact the service provider or exercise a particular right - without needing to hunt for information in webpages.

2) APIs AND NEW HEADERS FROM BROWSERS

Through APIs, web browsers provide a permissions-based model for websites to access resources such as camera, microphone, storage (e.g. cookies), and location. The use of this abstraction enables browsers and users to control and manage access to features at a local (i.e. specific website) and global (i.e. all websites) levels and to later inspect and change them through a settings or preference management interface. We argue for creation and utilisation of similar APIs to manage notices, consent, receipts, and other privacy related services.

Without a centrally defined common mechanism to generate, store, and verify information, browser support becomes invaluable given their role in identifying and using information declared within or by websites and their service providers. In addition, browsers are also well placed to identify and act in interactions taking place through HTTP signals (such as DNT and GPC), and can follow up communications with third-parties for privacy and receipt management in the background. Currently, we have fairly robust methods for authenticating identities of entities on the web through cryptographic methods (e.g. the HTTPS protocol) which can be repurposed to the context of receipts. This can be achieved by extending Public Key Infrastructure and SSL certificate mechanisms to assert legal identities for transparency, accountability, and data protection obligations.

Similarly, existing data storage methods and APIs through which browsers store preferences for websites, such as whether to permit access to location, can be extended to provide minimal functionality for storing preferences and receipts. Through this, users and websites can identify if the user has indicated their preference regarding consent previously on the website. Users can also change their initial decision while the website can decide to provide further interaction, such as a related notice, as a follow-up to the previous context. The mechanisms for such receipt handling mechanisms in browsers, their utilisation by websites, and the capabilities it provides to users needs further exploration.

3) SEMANTIC VOCABULARY FOR INTEROPERABLE INFORMATION

A standard for a receipt only indicates the fields or structure utilised to provide information. In order to enable auditability and transparency of information, and ensure

[37] While the iOS Settings provides an overview of tracking permissions given or requested by apps, and enables the user to toggle them collectively as well as individually, we argue that this setting is only restricted to 'tracking', which is not sufficiently defined or explored in terms of legal enforceability or the ability of the user to indicate or enforce such a consent outside of the device

its interoperability from service to users to third parties, some degree of semantics is necessary. For example, where two service providers indicate their purpose as '*Marketing*', there is ambiguity and uncertainty as to what it specifically refers to. Therefore, semantic vocabularies which permit machine-readable extensiblity along with interoperability are an important aspect of declaring such information which can conform to legal requirements and be used for exchanging information through receipts.

In addition to interoperability, semantic vocabularies are also necessary to achieve extension or specialisation of a concept to a particular context, domain, or use-case. For example, the use of '*Marketing*' as a purpose may be sufficient at a broad level, but a service provider or a user may wish to have more granular and specific expression such as '*Advertising*' or the even more specific description of '*Advertising about New Products*'. When dealing with consent and permissions, it is vastly useful to be able to connect the three concepts of '*Marketing*', '*Advertising*', and '*Advertising about New Products*' in a hierarchical fashion. This would enable handling them at arbitrary levels of granularity. Such hierarchies can assist in better user-management of privacy preferences such as when consent is requested for specific purposes (e.g. specific types of advertisements) and agents can match or compare these with user preferences that are declared at a broad level (e.g. no consent to any type of marketing). While the use of semantics for preference management is not novel, the possibilities it enables for interpreting what personal data processing the information within a receipt *entails* is a particularly interesting approach for further exploration.

Existing work, as described in Section III-B, has provided a variety of semantic vocabularies and approaches for indicating information related to consent. We suggest mechanisms such as DPV [33] which provide concepts based on legal requirements, are comprehensive, and represent a community agreement to the extent it is possible. Further work is needed to demonstrate its utilisation for (a) generating and using receipts, and (b) declaring annotations on webpages to markup relevant information.

V. USE-CASE IMPLEMENTATIONS

This section reports on the experience of implementing consent receipts across three common use-cases and demonstrating their feasibility and practicality by serving as '*proof-of-concept*' for each respective implementation.

The first use-case concerns websites where users enter some information via a form and indicate their preference for use of that information, such as for marketing. In such situations, the user interacts and expresses their choices regarding data usage and collection through the form and information it contains, as offered (directly) by the service provider. We show how the service provider can support and issue receipts for this scenario through the overall architecture consisting of: a secure protocol, embedding semantics in the website's HTML, collection and generation of receipts, and management of the lifecycle of the consent.

The second case concerns websites where users interact with a cookie or consent dialogue provided by a Consent Management Platform (CMP), which in turn offers a uniform interface and information based on the IAB's TCF standard across websites implementing that CMP's solutions. Here, we demonstrate the feasibility of receipts generated from interactions with consent/cookie dialogues by relying on the fact that the vast majority of consent banners found on the web are provided by CMPs and are based on the TCF v2.0 specification. For this implementation, we used the interface provided by CMP Usercentrics'[38] and created a browser extension (''addon'') that utilises JavaScript injections to extend the CMP's consent-handling code so that whenever the user makes a choice via the consent/cookie dialogue, a receipt is generated and stored in the background.

We note that this use-case, in practice, covers the browser signalling approaches such as ''Do Not Track'' since signalling is much simpler and, technically, unidirectional. When the browser automatically sends the signal, a receipt could be automatically generated partially using the techniques in the first use-case.

In our third implementation, we address the difficulties in interactions and expression of choices with IoT devices, such as the smart assistant Alexa, which only provides interactions via voice commands and does not have a visual interface (on device). To give a simple example, the user has to put extra effort in finding and reading the privacy notice and in a different device.

Our scenario consists of a user who requests Alexa to find when their garbage bin will be collected next. For this, Alexa requires the user's consent[39] to collect the required information (i.e. user's address) and to use it to check with the waste collection companies for their schedule by invoking a cloud-based application, after which it confirms with the user and books an appointment for bin collection. In the background, Alexa then generates and sends a consent receipt to the user by email as a record of this interaction.

A. CONSENT INTERACTIONS VIA FORMS ON WEBSITES

The first use-case addresses the lifecycle of consent on websites where the user provides information through a form, such as when creating an account or accessing a service. This use-case is based on the single moment of interaction where the user makes a choice regarding consent, such as through clicking a checkbox. After this consenting moment, common methods of providing options to change this choice is to visit account preference or settings and perform similarly interactions - conditional upon the user having an account with the service.

[38] https://usercentrics.com/.

[39] It can be argued that this scenario should utilise the legal basis of a contract or legitimate interest rather than consent based on the necessity of requiring an address to provide the garbage collection service. However, we focus on the principle of 'consent' as in assenting and the generation of a consent receipt for recording it.

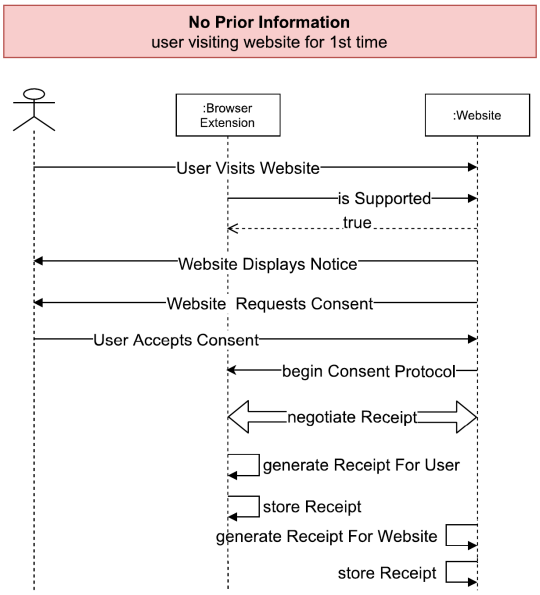

FIGURE 2. Signalling diagram for generating receipts on consent given.

Through our implementation, we seek to enrich this scenario with the use of consent receipts so as to provide the user with a record of their choice and to permit taking that record (i.e. store on a medium controlled by the user) with them after they leave the website. For this, we envision the browser, as the user-agent, natively supporting the consent receipt mechanisms and assisting the user in the receipt generation and management procedures. We implemented the required behaviour through a browser extension that handles receipt management on behalf of the user.

1) APPROACH AND IMPLEMENTATION

The process of generating a receipt is shown in the signalling diagram shown in figure 2 as: (i) the user visits a website; (ii) interacts and gives their consent; and (iii) is provided with a receipt. The browser extension checks for consent interactions (e.g. by looking for '*Agree*' button clicks) and once encountered checks if the website natively supports receipts (e.g. by looking for metadata declaring support for using a custom protocol). In both these instances, we assumed the identifiability of consent interactions and declarative support for consent receipts through ad-hoc mechanisms such as click-detection and metadata declarations as described in Section.IV. However, we found that no such mechanisms exist within the state of the art to identify or indicate a consent interaction taking place or a way for websites to indicate information or processes associated with consent. This reflects a critical lack of required infrastructure within the web ecosystem, which we have discussed in the earlier Section.IV.

Upon discovering that the website supports consent receipts, and after the user has given their consent, the extension engages with the website's server (representing the service provider) through a '*special protocol*' based on requirements for implementing secure receipts

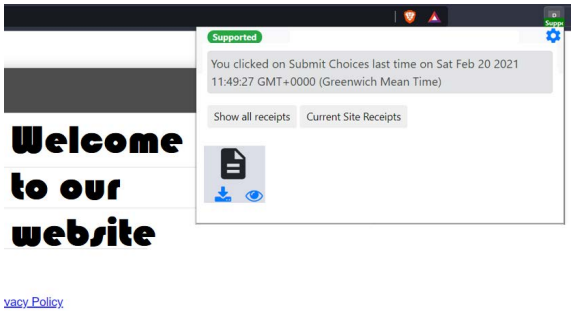

FIGURE 3. Browser extension generating a receipt for recording given consent.

(for details, reader is directed to [17]) to retrieve the required information and securely negotiate the consent receipt generation. In essence, the protocol assures that cryptographic information is exchanged that allows the local generation of signed receipts with the same factual information. This information includes details such as the privacy policy, nature of consent, method of data collection (HTML and JavaScript, in this case), and other pertinent details as discussed in Section IV. The receipts are thus made unforgeable and non-repudiable. After this step, the actual receipts are generated, and for the user, stored locally by the browser extension (as shown in Figure 3).

Our implementation supports other possibilities as well. First, the user could reject or refuse to provide consent, such as when the user reads the linked privacy policy and decides not to accept it due to their various data sharing concerns [15]. On refusal to consent, a similar sequence of actions is triggered with the only difference being that the receipt now records that consent was not given or was refused. It is important to note that a service provider may not actively support receipts showing the user has refused to consent, whether due to lack of legal motivation or deliberate choice. However, despite these setbacks, the receipt showing refusal to consent is a powerful artefact given that it can be used to prove the prohibition expressed by the user to process their personal data, and thereby challenge any illegal activities carried out by the service provider based on assumption or disregard of consent choices. Alternative mechanisms to ensure the receipt is still a verifiable artefact when the service provider does not participate is the use of a trusted third-party that signs the receipt in the role of a '*witness*' similar to the legal concepts of notary and claims [46].

We also considered scenarios associated with the user interacting within the context of that given consent, such as withdrawing it, or re-consenting or refreshing it. To explore such '*secondary*' and subsequent interactions, we considered the situation where conditions associated with the given consent have changed (e.g. some additional data is needed) and where the notice for such changes if provided when the user revisits the same website again. We addressed this case by requiring the website to annotate the webpage or consent elements with timestamps indicating the last effective change necessitating an acknowledgement or interaction from

the user. The browser extension then reads this timestamp and compares it with the information within stored receipts to determine whether the receipt has been generated prior to these changes, and if so, then whether the changes require notifying the user. In cases where the user is required to make a consent interaction again, a similar process to the first consent interaction is triggered by the website or add-on and a new receipt, superseding the previous one, is generated (as shown in Figure 4).

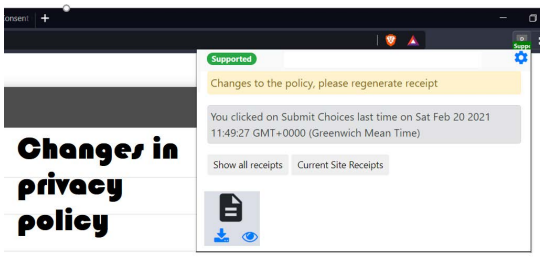

FIGURE 4. Use of receipts on subsequent consent requests following changes to the privacy policy.

For addressing the requirement of declaring required information as metadata within the webpage or consent dialogues, we utilised the existing HTML guidelines for declaring custom metadata[40] – see Listing 1). In the `<head>` element of the HTML, we declare `<meta name="pisp">` representing Privacy Information Service Point. Through this, the website or webpage informs the browser (extension) of, among other elements, the URL of the server to run the consent protocol, locations of privacy policy and JavaScript of the forms collecting the consent, the date of the most recent privacy policy, and so on. All these details are added (in the form of cryptographic digests) to the receipt. Through this we also addressed the issue of identifying the appropriate element for consent interactions by requiring the website to declare the element used to submit (e.g. 'Agree') a consent choice and used it to register an `on-click` event handled by the extension to execute the receipt generation and handling protocol upon its execution.

The use of HTML tag can also be helpful towards declarative transparency related to third-parties which are related to the consent interaction but not in control of the webpage i.e. they do not own or operate the website but receive consent from it. Here, the service provider, through its website, can indicate such Third Parties through the use of annotations and metadata as discussed earlier in Section IV. The extension can then utilise this information to communicate with the third-parties, identify whether they support receipts, and request receipts from those parties in the background. In cases the third-parties do not actively support receipts, the user-agent can generate a receipt solely on the user-side so as to keep a record of the interaction or forewarn the user prior to their choice about the lack of receipt availability. Should the Web embrace this practice, we expect the level of transparency

[40]https://html.spec.whatwg.org/multipage/dom.html#metadata-content

```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="utf-8">
  <meta name="pisp" content="ws://0.0.0.0:3100">
  <meta name="lastPolicyUpdateDate" content="2020-12-20">
  <script src="paecg.js"> </script>
  <script>
  var paecg=new PaECG(
    {'Submit':'Accept'},
    ['fname','lname','email'],
    [
      'http://0.0.0.0/js/one.js',
      'http://0.0.0.0/js/two.js' ],
    [
      'http://0.0.0.0/policy/one.html',
      'http://0.0.0.0/policy/two.html' ]);
  paecg.setup();
  </script>
```

Listing. 1. HTML tags providing information for receipts.

to dramatically increase. Even if users still do not read the entirety of their privacy policies, the number of receipts collected and the richness of their information will provide an incomparable degree of awareness, traceability, and accountability.

In our development of the browser extension, we envisioned further support for additional and typical user functionality such as downloading receipts and managing it through a dashboard, using receipt information for creating interactive visualisations for understanding privacy and data sharing practices, searching/sorting through receipts, and importing/exporting receipts from other devices or accounts. This was based on our observation that the core feature of generating receipts from a webpage and storing it through the browser (extension) user-agent represented functionality that can be practically invisible and unobtrusive to the user.

2) EVALUATION

We note that the protocol needs about 10 round-trips in terms of communication between the user-agent and the service provider's server. In our case, the size of consent receipt was small (1 kilobyte), and the process that handled the protocol and communication was executed in parallel to user activities. In other words, this is a background process that minimally affect usability on the main website. The total time for finishing these activities was less than 1 second. Through this, we found receipts to be efficiently handled in the background in a manner that produced no disruptions to the user's actions or interactions in the foreground. Considering the generation of receipts is an infrequent activity, we do not expect any usability hurdle in their usage. For additional evaluation metrics, see [17].

B. CONSENT MANAGEMENT PLATFORMS

The second scenario consists of consent/cookie banners typically served by Third parties as a Consent Management Platforms (CMP). These organisations dominantly follow the guidelines (and implementation) of the IAB TCF v2.0 framework for consent.

We used a commercially available platform of a well-known CMP, Usercentrics and extended their functionality with consent receipts. A simple webpage was created that displayed a familiar cookie banner as shown in Figure 5. This represents a practical and typical situation on the web, where service providers utilise CMPs to handle consent interactions by deploying their dialogues and banners on their websites. Given that some CMPs already implement a form of consent receipt to record the events associated with consent (see Section III-C), our implementation demonstrates further use of such mechanisms to generate the receipts on the user-side and with cryptographic guarantees to make them actionable artefacts.

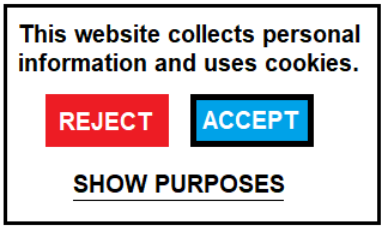

FIGURE 5. Test cookie banner.

1) APPROACH AND IMPLEMENTATION

Similar to the previous use-case, we utilised a browser extension to handle consent and receipts with the following modifications made to the consent management mechanisms (see Figure 6):

1) User visits a website and is presented with a consent/cookie dialogue provided by the CMP, which utilises the IAB TCF v2.0 framework through a script loaded and executed locally;
2) The user accepts or declines using the options provided in the consent dialogue. The CMP code sends the choice expressed by the user and its related information to the CMP or service provider (as configured by the service provider);
3) The server (CMP or service provider) sends a confirmation to the local CMP code, and a consent receipt is generated (on server or locally) which is then sent to the respective server(s) and user's browser for storage;
4) The extension on the browser detects the generated receipt and stores it locally (see Figure 7). It further sends a confirmation of reception of receipt to the server(s) for CMP and/or service provider.

In these interactions, we note that we deliberately ignored the key function of IAB's framework which is centred on federated data sharing through the use of its TCF specification for implementing real-time bidding for web advertisements, which enables the collection of a vast amount of personal information that involves several third-parties [25], [47]. Instead, we chose to focus our work on the component that manages consent, i.e. the role of CMP as a data processor or mediator in the process of receipt generation.

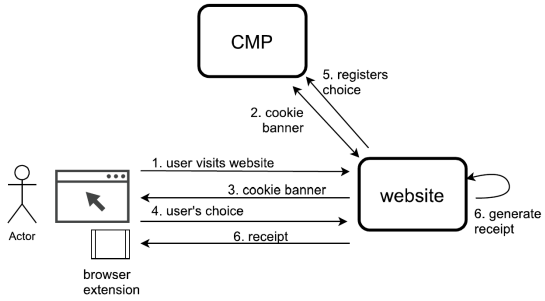

FIGURE 6. Integration of receipts with cookie banners.

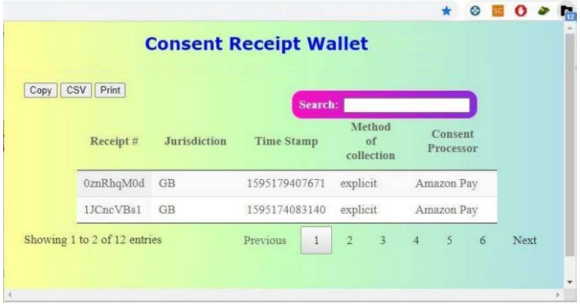

FIGURE 7. Browser extension to store receipts.

Similar to the experience in first use-case implementation, we found the browser extension handles receipts in the background with no disruption to the user. The difference in the information and communication processes was minor in terms of time and processing requirements, and we found an additional duration of approximately 500ms (discounting round-trip times) was needed for the completion of receipt generation and storage process.

2) EVALUATION

Similarly to the previous case, the impact on usability is minimal since any existing latency will be due to the Consent Management transactions themselves and the actual process of generating the receipt runs in the background. We ran both client (Firefox browser) and webserver on the same laptop (mid-range machine: core i5, 16GB RAM) so to minimise network latency. We repeated measurements 50 times and calculated averages.

As Figure 8 shows, the overall process runs in under 1 sec (average 717ms with a max of 1562ms). Additional functions such as storage or generation of the receipt are under 3ms. To note that this process is embedded

C. AMAZON ALEXA VOICE-ACTIVATED HOME ASSISTANT

In this last use-case for receipts, we demonstrate how they can be used in IoT devices with user interface constraints. Specifically, we implemented receipts for the Amazon Alexa voice-assistant. Figure 9 shows the overall architecture of our implementation. The top part of the figure shows the software development in Amazon Web Services (AWS) and the bottom shows how we extended the functionality in our own server in order to support receipts. An application for Amazon Alexa relies on the third-party extension mechanism

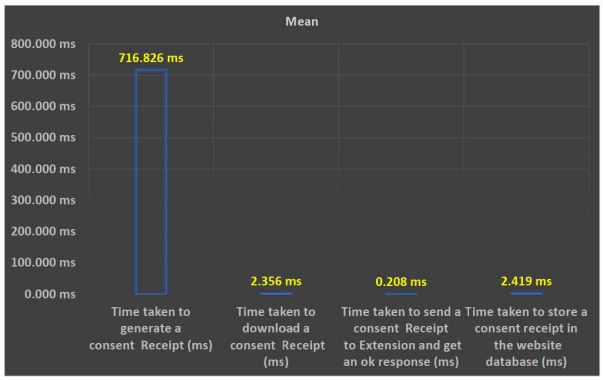

FIGURE 8. Integration of receipts with cookie banners.

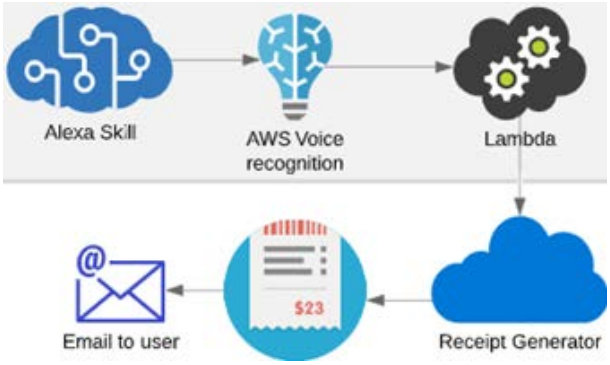

FIGURE 9. Implementing receipts in Alexa.

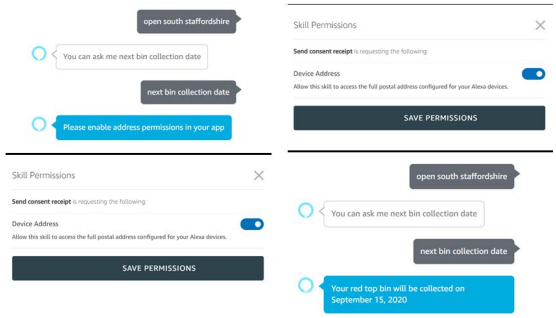

FIGURE 10. User interface in Alexa.

called 'Skills'. To simplify, one configures the trigger words in a newly created Alexa skill. If the device recognises the trigger words, it sends a request for further processing to the configured server, typically executed in an Amazon AWS where pre-configured custom code is hosted and run.

Our test application consisted of booking garbage collection from a City Council. As shown in Figure 10-top (transcripts of spoken messages), the user would start the Alexa application by saying "open" and name the application (in our case, a City Council in England). The voice assistant accepts the request but asks the user to first accept the Privacy Policy and personal data sharing settings. Note that these permissions are not intended to be for Amazon directly, but instead allow Amazon to share personal data with a third-party.

The user has to use a computer to enable this setting as shown in Figure 10-middle at least because Alexa, it seems, will not accept authentication using voice. Once third-party sharing has been enabled, the original voice-request can now be completed. Figure 10-bottom shows the original request and Alexa contacting the third-party provider. In the process, the application supporting this skill for Alexa will generate a consent receipt that is sent by email to the user. After this, the garbage collection is now scheduled and the user receives a confirmation.

VI. CONCLUSION

This paper introduced, characterised and outlined the usefulness and benefits of 'consent receipts' to assist users, service providers, and authorities regarding the transparency and auditability of consent. We argued that consent receipts have the potential to bring a different paradigm to personal data on the Web by providing an unobtrusive and intuitive way for recording their interactions similar to grocery receipts. We demonstrated the feasibility and simplicity of generating consent receipts through three use-cases covering different but widely relevant scenarios: accepting requests on a website, consenting through CMPs based on IAB TCF framework, and interactions with the Amazon Alexa voice-assistant.

Our implementation outlines the technical practicalities involved and shows that the onus of effort in creating and providing receipts is mostly on the service providers and only marginally on the user. This works not only towards reducing the burden on users for managing their privacy interactions, but also provides a way for service providers to document and maintain consent records for compliance.

PRACTICALITY OF CONSENT RECEIPTS

This work raises a number of questions regarding the legality, structure, and implementation of consent receipts across platforms and jurisdictions. We outline a few that also serve as avenues for future work involving receipts. First, it is important to look at these from an inter-disciplinary perspective given that requirements for managing consent are not limited to the technical and legal communities, but also involves usability (as HCI), security, ethics and business models.

For receipts to be utilised as a supporting document in the settlement of dispute and as evidence of malpractice, it is important to have support[41] from the authorities regarding their legal effectiveness. The recent clarification of GPC as an enforceable mechanism and the upcoming (and ongoing) changes to privacy and data protection laws across both USA and EU provide opportunities for achieving this. Other issues in this also include specifying international data transfers, assuring the identity of the entities such as recipients, use of receipts in exercising rights, and codifying data collection and sharing practices.

[41] Support can be in the form of guidelines encouraging adoption, codes of conduct requiring records of consent, encouragement to utilise standards, and comments on validity or usefulness of receipts through case law.

Second, the implementations we demonstrated can be considered prototypes and early iterations. Even though we found the software components and processes intuitive and easy to run, this needs to be confirmed through more rigorous tests that involve both scale and functionality and are carried out in more scenarios and devices/platforms. Many other research questions are also relevant and encourage more attention and research from the community. Issues such as handling non-supporting websites is an important hurdle to cross for receipts. For this, we find the use of third-party services that manage receipts or act as notaries/witnesses an interesting solution to pursue. Another relevant issue is the study of assurances offered by receipts, and how feasible these can be through time where legal requirements change and companies are merged or bought.

FURTHER DEVELOPMENT OF CONSENT RECEIPTS

The future research and work regarding consent receipts is promising given that we might see the push for CMPs and websites to utilise the ISO/IEC 29184:2020 [37] standard for notice and consent. ISO/IEC 29184 provides the motivation to produce a machine-readable receipt, while the ongoing effort and involvement of nations and authorities in developing ISO/IEC 27560 [48] as a specification for consent records points towards its eventual coming on the horizon.

Based on these, future work also consists of analysing these as well as other existing standards and relevant research in terms of information and processes to create a harmonised specification for the development and implementation of consent receipts. Additionally, receipts need to further enhanced in terms of security of information, actors, and the identification and mitigation of threat models. This needs to be a smooth and transparent process for ease of use by the users, similar to the way digital certificates are utilised on the web for secure communication, and where problematic cases are highlighted with large warnings.

Consent receipts that store personal data, especially of sensitive nature, need further work that investigates how such information should be secured in terms of its storage and communication. For this, receipts in their entirety, or the information within them can be obfuscated or protected through measures that utilise anonymisation or encryption with strong cryptographic guarantees. Doing so can permit safer sharing of the receipt with another party, such as for verification or demonstration purposes, or assist in publishing it to the public, for example as proof of consent to public data usage.

The above exercises are necessary for the eventual adoption and acceptance of consent receipts socially as well as within software and for it to become a method for ensuring and demonstrating legal and social accountability. In this, is is important to demonstrate sufficiency regarding security guarantees it provides, as well as the interoperability and commonality of information based on adherence to ISO/IEC standards.

We remain optimistic that receipts, as a concept, will be a point of contention and eventual adoption, regardless of laws becoming increasingly pragmatic and pro-consumer or as an industry-wide code of conduct.

ACKNOWLEDGMENT

The authors would like to thank Tregon Henry and Muhammad Waqas for their support in developing the proof of concepts, and also would like to thank UserCentrics, a Consent Management Provider for the support and access to their platform.

REFERENCES

[1] European Parliament and Council of the European Union, "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)," *Off. J. Eur. Union*, vol. L119, May 2016.

[2] J. Sørensen and S. Kosta, "Before and after GDPR: The changes in third party presence at public and private European websites," in *Proc. World Wide Web Conf.*, New York, NY, USA, 2019, pp. 1590–1600.

[3] M. Hils, D. W. Woods, and R. Böhme, "Measuring the emergence of consent management on the web," in *Proc. ACM Internet Meas. Conf.*, Virtual Event USA, Oct. 2020, pp. 317–332.

[4] D. Machuletz and R. Böhme, "Multiple purposes, multiple problems: A user study of consent dialogs after GDPR," *Proc. Privacy Enhancing Technol.*, vol. 2020, no. 2, pp. 481–498, Apr. 2020.

[5] C. M. Gray, C. Santos, N. Bielova, M. Toth, and D. Clifford, "Dark patterns and the legal requirements of consent banners: An interaction criticism perspective," in *Proc. CHI Conf. Hum. Factors Comput. Syst.*, May 2021, pp. 1–18.

[6] 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," *Technol. Regulation*, vol. 2020, pp. 91–135, Dec. 2020.

[7] C. Matte, N. Bielova, and C. Santos, "Do cookie banners respect my choice?" in *Proc. 41st IEEE Symp. Secur. Privacy*, May 2020, p. 19.

[8] C. Utz, M. Degeling, S. Fahl, F. Schaub, and T. Holz, "(Un)informed consent: Studying GDPR consent notices in the field," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, London, U.K., Nov. 2019, p. 18.

[9] M. Kretschmer, J. Pennekamp, and K. Wehrle, "Cookie banners and privacy policies: Measuring the impact of the GDPR on the web," *ACM Trans. Web*, vol. 15, no. 4, pp. 20:1–20:42, Jul. 2021.

[10] T. H. Soe, O. E. Nordberg, F. Guribye, and M. Slavkovik, "Circumvention by design—Dark patterns in cookie consents for online news outlets," 2020, *arXiv:2006.13985*.

[11] I. Fouad, C. Santos, F. Al Kassar, N. Bielova, and S. Calzavara, "On compliance of cookie purposes with the purpose specification principle," in *Proc. IEEE Eur. Symp. Secur. Privacy Workshops (EuroS&PW)*, Sep. 2020, pp. 326–333.

[12] M. Nouwens, I. Liccardi, M. Veale, D. Karger, and L. Kagal, "Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence," in *Proc. CHI Conf. Hum. Factors Comput. Syst.*, Apr. 2020, pp. 1–13.

[13] M. Fassl, L. T. Gröber, and K. Krombholz, "Stop the consent theater," in *Proc. Extended Abstr. CHI Conf. Hum. Factors Comput. Syst.*, Yokohama, Japan, May 2021, pp. 1–7.

[14] S. Human and F. Cech, "A human-centric perspective on digital consenting: The case of GAFAM," in *Proc. Hum. Centred Intell. Syst.*, Split, Croatia, 2020, 2020.

[15] J. A. Obar and A. Oeldorf-Hirsch, "The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services," *Inf., Commun. Soc.*, vol. 23, no. 1, pp. 128–147, Jan. 2020.

[16] R. Bailey, S. Parsheera, F. Rahman, and R. Sane, "Disclosures in privacy policies: Does 'notice and consent' work?" *Nat. Inst. Public Finance Policy (NIPFP)*, New Delhi, India, Nov. 2018, paper. 246.

[17] V. Jesus, "Towards an accountable web of personal information: The web-of-receipts," *IEEE Access*, vol. 8, pp. 25383–25394, 2020.

[18] T. Urban, D. Tatang, M. Degeling, T. Holz, and N. Pohlmann, "A study on subject data access in online advertising after the GDPR," in *Data Privacy Management, Cryptocurrencies and Blockchain Technology* (Lecture Notes in Computer Science), C. Pérez-Solà, G. Navarro-Arribas, A. Biryukov, and J. Garcia-Alfaro, Eds. Cham, Switzerland: Springer, 2019, pp. 61–79.

[19] J. L. Kröger, J. Lindemann, and D. Herrmann, "How do app vendors respond to subject access requests? A longitudinal privacy study on iOS and Android apps," in *Proc. 15th Int. Conf. Availability, Rel. Secur.*, New York, NY, USA, Aug. 2020, pp. 1–10.

[20] M. D. Martino, P. Robyns, W. Weyts, P. Quax, W. Lamotte, and K. Andries, "Personal information leakage by abusing the GDPR 'right of access'," in *Proc. 15th Symp. Usable Privacy Secur.* Santa Clara, CA, USA: USENIX Association, Aug. 2019, pp. 371–385.

[21] M. Veale, R. Binns, and J. Ausloos, "When data protection by design and data subject rights clash," *Int. Data Privacy Law*, vol. 8, no. 2, pp. 105–123, Apr. 2018.

[22] J. Ausloos, M. Veale, and R. Mahieu, "Getting data subject rights right," *J. Intellectual Property, Inf. Technol. Electron. Commerce Law*, vol. 10, 2019.

[23] R. Wenning and S. Kirrane, "Compliance using metadata," in *Semantic Applications: Methodology, Technology, Corporate Use*, T. Hoppe, B. Humm, and A. Reibold, Eds. Berlin, Germany: Springer, 2018, pp. 31–45.

[24] J. Turow and C. J. Hoofnagle, *Opinion | Mark Zuckerberg's Delusion of Consumer Consent*. New York, NY, USA: The New York Times, Jan. 2019.

[25] N. Lomas, "Google and IAB ad category lists show 'massive leakage of highly intimate data,' GDPR complaint claims," TechCrunch, Tech. Rep., Jan. 2019. Accessed: Jan. 4, 2021. [Online]. Available: https://techcrunch.com

[26] A. Kurteva, T. R. Chhetri, H. J. Pandit, and A. Fensel, "Consent through the lens of semantics: State of the art survey and best practices," *Semantic Web*, pp. 1–27, Sep. 2021.

[27] P. A. Bonatti, S. Kirrane, I. M. Petrova, and L. Sauro, "Machine understandable policies and GDPR compliance checking," *Künstliche Intelligenz*, vol. 34, no. 3, pp. 303–315, Sep. 2020.

[28] M. Palmirani, M. Martoni, A. Rossi, C. Bartolini, and L. Robaldo, "PrOnto: Privacy ontology for legal compliance," in *Proc. 18th Eur. Conf. Digit. Government*, 2018, p. 10.

[29] G. Lioudakis and D. Cascone, "D3.1 compliance ontology," BPR4GDPR H2020 Project Deliverable, Tech. Rep. D3.1, Feb. 2019.

[30] N. Gol Mohammadi, J. Leicht, N. Ulfat-Bunyadi, and M. Heisel, "Privacy policy specification framework for addressing end-users' privacy requirements," in *Trust, Privacy and Security in Digital Business*, S. Gritzalis, E. R. Weippl, S. K. Katsikas, G. Anderst-Kotsis, A. M. Tjoa, and I. Khalil, Eds., vol. 11711. Cham, Switzerland: Springer, 2019, pp. 46–62.

[31] P. A. Bonatti, L. Sauro, and J. Langens, "Representing consent and policies for compliance," in *Proc. IEEE Eur. Symp. Secur. Privacy Workshops (EuroS&PW)*, Sep. 2021, pp. 283–291.

[32] H. J. Pandit, C. Debruyne, D. O'Sullivan, and D. Lewis, "GConsent—A consent ontology based on the GDPR," in *The Semantic Web* (Lecture Notes in Computer Science), P. Hitzler, M. Fernández, K. Janowicz, A. Zaveri, A. J. Gray, V. Lopez, A. Haller, and K. Hammar, Eds. Cham, Switzerland: Springer, 2019, pp. 270–282.

[33] H. J. Pandit, A. Polleres, B. Bos, R. Brennan, B. Bruegger, F. J. Ekaputra, J. D. Fernández, R. G. Hamed, M. Lizar, E. Schlehahn, S. Steyskal, and R. Wenning, "Creating A vocabulary for data privacy," in *Proc. 18th Int. Conf. Ontologies, DataBases, Appl. Semantics*, Rhodes, Greece, 2019, p. 17.

[34] M. Nati, "Personal data receipts: How transparency increases consumer trust," Catapult Digital, London, U.K., Tech. Rep., Mar. 2018.

[35] K. A. Barday, J. B. Brannon, J. L. Sabourin, M. S. Karanjkar, K. Jones, and A. R. Beaumont, "Consent receipt management systems and related methods," U.S. Patent 10 678 945 B2, Sep. 24, 2020.

[36] M. Lizar and D. Turner, "Consent receipt specification V1.1.0," Kantara Initiative, Tech. Rep. 1.1.0, 2017. [Online]. Available: https://kantarainitiative.org

[37] *ISO/IEC 29184/2020 Information Technology—Online Privacy Notices and Consent*, ISO/IEC, Jun. 2020.

[38] H. J. Pandit and G. P. Krog, "Comparison of notice requirements for consent between ISO/IEC 29184:2020 and general data protection regulation," *J. Data Protection Privacy*, vol. 4, no. 2, pp. 193–204, 2021.

[39] M. Bialke, T. Bahls, L. Geidel, H. Rau, A. Blumentritt, S. Pasewald, R. Wolff, J. Steinmann, T. Bronsch, B. Bergh, G. Tremper, M. Lablans, F. Ückert, S. Lang, T. Idris, and W. Hoffmann, "MAGIC: Once upon a time in consent management—A FHIR tale," *J. Translational Med.*, vol. 16, no. 1, pp. 1–11, Dec. 2018.

[40] "Assembly bill no. 375 chapter 55: An act to add title 1.81.5 (commencing with section 1798.100)—Part 4 of division 3 of the civil code, relating to privacy," *California State Legislature*, Jun. 2018.

[41] "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)," Jan. 2017.

[42] T. E. B. A. Claesson, "Out of Control—A review of data sharing by popular mobile apps," Norwegian Consumer Council, Oslo, Norway, Tech. Rep. , Jan. 2021.

[43] C. Boniface, I. Fouad, N. Bielova, C. Lauradoux, and C. Santos, "Security analysis of subject access request procedures—How to authenticate data subjects safely when they request for their data," in *Privacy Technologies and Policy* (Lecture Notes in Computer Science). Cham, Switzerland: Springer, Jun. 2019, pp. 1–20.

[44] V. Jesus and S. Mustare, "I did not accept that: Demonstrating consent in online collection of personal data," in *Trust, Privacy and Security in Digital Business*, vol. 11711, S. Gritzalis, E. R. Weippl, S. K. Katsikas, G. Anderst-Kotsis, A. M. Tjoa, and I. Khalil, Eds. Cham, Switzerland: Springer, 2019, pp. 33–45.

[45] *iOS 14.5 Opt-in Rate—Daily Updates Since Launch | Flurry*. Accessed: Jan. 4, 2021. [Online]. Available: https://www.flurry.com/blog/ios-14-5-opt-in-rate-att-restricted-app-tracking-transparency-worldwide-us-daily-latest-update/

[46] H. J. Pandit, V. Jesus, S. Ammai, M. Lizar, and S. D'Agostino, "Role of identity, identification, and receipts for consent," in *Open Identity Summit*. Bonn, Germany: German Informatics Society, 2021.

[47] M. Veale and F. Z. Borgesius, "Adtech and real-time bidding under European data protection law," *German Law J.*, Jul. 2021.

[48] *ISO/IEC WD TS 27560 Privacy Technologies Consent Record Information Structure*, ISO/IEC, 2021.

VITOR JESUS received the Ph.D. degree in computer science and industry certifications in cybersecurity and data privacy. He is currently a Lecturer with Aston University, U.K. He has 20 years of experience between industry and academia, having held lead technical roles at large and small organizations. He is currently a Consultant with a special interest in working with start-ups and small businesses looking to different approaches to trust, security, and privacy. His research interests include computer science and trust, notably cybersecurity, and privacy. He is the Founder of PrivDash with a new approach to user-centred data protection, the mentor and a lead in several funded projects in security and privacy, and an Active Member in communities and standards, such as BSI/ISO, U.K.'s SPRITE+ Network, IoTSF, or Kantara Initiative. He is a frequent author and a reviewer in conferences and journals, and participant in discussions, panels, and events related to consent.

HARSHVARDHAN J. PANDIT received the Ph.D. degree in computer science from the Trinity College Dublin. He explored the application of linked data and semantic web technologies towards GDPR compliance, with a particular focus on consent and provenance. He is currently a Postdoctoral Researcher with the Trinity College Dublin, exploring the application of semantics to real-world challenges associated with privacy risks, legal and regulatory compliance, and consent. He currently co-chairs the W3C Data Privacy Vocabularies and Controls Community Group (DPVCG)—which works on creating interoperable vocabularies for personal data handling based on legal and practical requirements and the W3C Consent Community Group (CONSENT), which has recently started its work on improving the experience of digital consent and consenting. He also contributes to ISO/IEC efforts on consent and privacy standardization through the National Standards Authority of Ireland.