The EU's proposed new cookie rules[1]: digital advertising, European media, and consumer access to online news, other content and services

The European Union is currently considering a proposed regulation on ePrivacy that, unless amended, will have serious negative impacts on the digital advertising industry, on European media, and ultimately on European citizens' access to information and other online content and services. Member States need to engage to ensure a rational outcome that protects the rights of companies, media and consumers.

ePrivacy in the context of Europe's data protection reform and Digital Single Market

In December 2015, after four years of difficult negotiations, the EU agreed its General Data Protection Regulation (GDPR). The GDPR introduces strong consumer protections online, and a range of new obligations that both companies and data protection authorities are still trying to understand and implement[2]. It radically alters information disclosure requirements, vastly improving consumer visibility as to who is processing personal data and for what purposes. It provides for steep fines of up to four percent of global turnover, or €20,000,000 (whichever is higher) for companies found to be in breach of the law. Its scope is broader than that of the 1995 Data Protection Directive, which it replaced – it clearly covers cookies and other online identifiers.

The Regulation introduced such complex and comprehensive changes in comparison with the 1995 Directive, that a two-year implementation period was laid down. It will be enforced only as from 25 May 2018.

Yet less than a year after the adoption of the GDPR, and without waiting to see whether the GDPR appeared to leave any gaps in consumer protection, the European Commission's DG CONNECT issued another draft law that includes provisions that cover much the same ground (indeed, the new proposal is based on the very same Article of the Treaty [3]). The new draft law is the proposed ePrivacy Regulation. It is an update of the famous Cookie Directive of 2009.

---

[1] 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 Communication).

[2] Commission Vice President Andrus Ansip and Justice and Home Affairs Commissioner Vera Jourovà welcomed this major reform of the Union's horizontal data protection rules. The new Regulation would "make Europe fit for the digital age", with new consumer protections online such as the "right to be forgotten", and a higher legal bar for automated decisions based on profiling that might have significant negative effects on users.

[3] Article 16 of the Treaty on the Functioning of the European Union, on the right to the protection of personal data.

Negative impacts on the digital advertising industry

The new ePrivacy proposal would reduce the multiple legal bases for data processing laid down in the GDPR to only one – consent – and consent as defined in the GDPR. A consent-only regime would negatively impact the digital advertising industry in several ways:

- Consent-only means "opt-out" business models need to be rethought

  Virtually all interactions between the supplier of an online service and a user's terminal device require the use of storage and processing capabilities of, or the accessing of information on, that terminal device. As a consequence, if the proposed ePrivacy regulation were adopted without amendment, virtually all Internet activities would fall in-scope and therefore be subject to consent. Websites, apps and providers of other online services would be deprived of other legal bases foreseen in the General Data Protection Regulation (GDPR) that was adopted only last year, notably the legitimate interest (opt-out) legal basis.[4] This means that business models built on the use of the legitimate interest legal basis – a legal basis that four years of negotiations in the European Parliament and Council found to provide strong consumer protection and accountability for data controllers – will need to be rethought.

- Consent-only penalises Third Parties

  'Third parties' such as ad tech companies with no direct link to the end-user will be unable to collect consent, even assuming their data processing is fully in line with these conditions. Instead, consent will need to be organised on their behalf by websites or apps that do have that direct link. This paradigm hands a significant advantage to vertically-integrated, consumer-facing platforms, many of which are not EU-based, who *do* have the direct link to the user and so are better-placed to organise consent, and who also act as third parties in the digital advertising delivery chain, competing with the EU-based companies who are purely ad tech/third parties. The competitive advantage accruing to these vertically-integrated companies, who are also able to leverage data derived from their first-party, consumer-facing businesses, will further aggravate what some say are imbalances in the existing market structure.

- Consent under GDPR comes with heavy conditionality and may simply not work

  Ironically, since consent under the ePrivacy regulation will mean consent as defined in the GDPR, it may not even work for the vertically-integrated companies or for successful publishers acting as first parties. Consent under the GDPR comes with important constraints, mainly to do with the fact that in order to be valid as a legal basis, it must be "freely given". Consent is considered *not* to be freely given if the user could be considered to suffer "detriment" if he or she could not access the service, or if he or she could be considered to be in a situation of "imbalance" vis-à-vis the supplier of the online service, or if accessing the service required the user to consent to any data processing that was not necessary to deliver the service from a technical point of view. As noted above, if the consent is not "freely given" then it may not be used as a legal basis by the provider of the online service. And if consent is the only legal basis foreseen in the law, and it is not available, then the processing simply may not take place.

[4] The GDPR will be enforced as from 25 May 2018.

- Prior information requirement will "break" programmatic trading

  Consent under the GDPR must be "informed", that is, the user consenting to the processing must have *prior* information as to the identity of the data controller processing his or her personal data and the purposes of the processing.[5] As it is technically impossible for the user to have prior information about every data controller involved in a real-time bidding (RTB) scenario, programmatic trading, the area of fastest growth in digital advertising spend, would seem, at least *prima facie*, to be incompatible with consent under GDPR – and, as noted above, if a future ePrivacy Regulation makes virtually all interactions with the Internet subject solely to the consent legal basis, and consent is unavailable, then there will be no legal be no basis for such processing to take place or for media to monetise their content in this way.

Negative impacts on European media

Since, for the reasons outlined above, media are likely to suffer from diminished advertising revenue streams and an inability to customize content for individual users, the future regulation will inevitably lead to an impoverishment of the media landscape and aggravate the already serious problem of excessive media concentration in Europe.

Negative impacts on European citizens

The inevitable consequences of a future regulation making it more difficult for media to monetise their content will be a less rich range of information sources for citizens to choose from and potentially less variety and quality content produced by each media outlet, obviously an undesirable development in any democratic society.

The way forward

The foregoing negative impacts can still be avoided by either deleting the relevant provisions of the proposed regulation altogether, or by amending them to ensure 100% alignment with the General Data Protection Regulation adopted last year. This would mean ensuring that media and companies involved in delivering digital advertising had access to all the legal bases laid down in that Regulation. Practically, this could be achieved either inserting a new exception in Article 8 for any data processing that would satisfy the conditions for legality under the GDPR. Such modifications are urgently needed.

In addition, in light of the constraints on consent under the GDPR discussed above, and to ensure that those suppliers of online services for whom consent is the most appropriate legal basis (e.g. because they have users who are already logged in and so are collecting more data anyway) are actually able to leverage it, language from the 2009 Directive clarifying that access content may be conditional on consent for data processing should be restored.

Amendments that would achieve these objectives are annexed to this paper.

[5] See recitals 32 and 42 of the General Data Protection Regulation.

Reason for redactions: protection of personal data, in accordance with Regulation (EC) 45/2001.

For further information, please contact [redacted] or [redacted].

June 2017

ANNEX

Article 8 *Protection of information stored in and related to end-users' terminal equipment*	***Article 8*** *Protection of information stored in and related to end-users' terminal equipment*
OPTION NO. 1	
1. The use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment, including about its software and hardware, other than by the end-user concerned shall be prohibited, except on the following grounds: (a) it is necessary for the sole purpose of carrying out the transmission of an electronic communication over an electronic communications network; or (b) the end-user has given his or her consent; or (c) it is necessary for providing an information society service requested by the end-user; or if it is necessary for web audience measuring, provided that such measurement is carried out the provider of the information society service requested by the end-user.	1. The use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment, including about its software and hardware, other than by the end-user concerned shall be ***lawful if such use is performed on the basis of the consent of the end-user or some other legitimate basis laid down by law, in accordance with Regulation (EU) 2016/679.*** ~~**prohibited, except on the following grounds:**~~ ~~**(a) it is necessary for the sole purpose of carrying out the transmission of an electronic communication over an electronic communications network; or**~~ ~~**(b) the end-user has given his or her consent; or**~~ ~~**(c) it is necessary for providing an information society service requested by the end-user; or**~~ ~~**(d) if it is necessary for web audience measuring, provided that such measurement is carried out the provider of the information society service requested by the end-user.**~~

This amendment would perfectly align the "cookie provision" of the proposed ePrivacy regulation with the General Data Protection Regulation (GDPR) by extending the rules of the GDPR beyond personal data to any processing covered by the ePrivacy Regulation. This approach would provide for the highest degree of legal certainty and consistency for both businesses and consumers, since any modification of the legal bases of the GDPR would 'automatically' apply also to the future ePrivacy regulation.

In effect, this change would maintain the level of protection of personal data laid down in the GDPR and extend data protection rules to any information, whether personal or not, that relates to the terminal equipment of end-users.

Article 8 *Protection of information stored in and related to end-users' terminal equipment*	*Article 8* *Protection of information stored in and related to end-users' terminal equipment*
OPTION NO. 2	
1. The use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment, including about its software and hardware, other than by the end-user concerned shall be prohibited, except on the following grounds: (a) it is necessary for the sole purpose of carrying out the transmission of an electronic communication over an electronic communications network; or (b) the end-user has given his or her consent; or (c) it is necessary for providing an information society service requested by the end-user; or (d) if it is necessary for web audience measuring, provided that such measurement is carried out the provider of the information society service requested by the end-user.	1. The use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment, including about its software and hardware, other than by the end-user concerned shall be prohibited, except on the following grounds: (a) it is necessary for the sole purpose of carrying out the transmission of an electronic communication over an electronic communications network; or (b) the end-user has given his or her consent; or (c) it is necessary for providing an information society service requested by the end-user; or (d) if it is necessary for ~~**web**~~ audience measuring ***or for scientific and statistical research purposes; or*** ~~**, provided that such measurement is carried out the provider of the information society service requested by the end-user.**~~ (e) ***[NEW] if it is necessary for pursuing a legitimate purpose and the person responsible undertakes to comply with specific privacy safeguards listed in paragraph 1c; or*** (f) ***[NEW] it is necessary to maintain or restore the security of information society services, or detect technical faults and/or errors in the functioning of information society services, for the duration necessary for that purpose.***

This amendment would align the ePrivacy proposal with the General Data Protection Regulation (GDPR) in a similar way to Option No. 1 above, but by explicitly calling out each of the various legal bases for the processing of personal data that are currently foreseen in the GDPR.

	<u>In case of Option 2:</u> ***1c. (new) For the purpose of point (e) of paragraph 1 the following specific privacy safeguards apply:*** ***(a) no data relating to the content of any user communications is collected;*** ***(b) the responsible person has put in place appropriate technical measures, such as pseudonymisation or encryption.*** ***(c) no effort is made or technique is applied to re-identify the end-user without his or her consent;*** ***(d) the data processed do not constitute special categories of personal data as defined by Article 9 of Regulation (EU) 2016/679; and*** ***(e) the responsible person has carried out a data protection impact assessment as defined by Article 35 of Regulation (EU) 2016/679.***

This new provision would specify under which conditions information stored in and related to end-users' terminal equipment may be processed without consent under the new exception of Art. 8(1)(f) in addition to the requirement of only processing anonymised or pseudonymised data.

This addition would only be necessary if "Option 2" for Art. 8(1) is pursued.

	<u>In case of Option 2:</u> ***1d. (new) The Commission shall be empowered to adopt delegated acts to specify additional privacy safeguards, including differentiation of privacy safeguards on the basis of risks associated with the processing.***

This new provision would empower the European Commission to specify additional privacy safeguards under the new provision Art. 9(1c) to ensure the long term effectiveness of a technology-centric provision.

This addition would only be necessary if "Option 2" for Art. 8(1) is pursued.

Article 9 *Consent*	***Article 9*** ***Consent***
1. The definition of and conditions for consent provided for under Articles 4(11) and 7 of Regulation (EU) 2016/679/EU shall apply.	1. The definition of and conditions for consent provided for under Articles 4(11) and 7 of Regulation (EU) 2016/679/EU shall apply.
	1a. (NEW) Article 7(4) of Regulation (EU) 2016/679/EU shall not mean that the provider of an information society service is prohibited from making access to its service conditional on the end-user's consent.

This amendment would maintain the clarification of the existing ePrivacy Directive (Recital 25) that access to an online service may be made conditional on the well-informed consent of a user, for example to provide interest-based advertising.

Recitals 20, 21, 22, 24	Proposed amendments
(20) Terminal equipment of end-users of electronic communications networks and any information relating to the usage of such terminal equipment, whether in particular is stored in or emitted by such equipment, requested from or processed in order to enable it to connect to another device and or network equipment, are part of the private sphere of the end-users requiring protection under the Charter of Fundamental Rights of the European Union and the European Convention for the Protection of Human Rights and Fundamental Freedoms. Given that such equipment contains or processes information that may reveal details of an individual's emotional, political, social complexities, including the content of communications, pictures, the location of individuals by accessing the device's GPS capabilities, contact lists, and other information already stored in the device, the information related to such equipment requires enhanced privacy protection. Furthermore, the so-called spyware, web bugs, hidden identifiers, tracking cookies and other similar unwanted tracking tools can enter end-user's terminal equipment without their knowledge in order to gain access to information, to store hidden information and to trace the activities. Information related to the end-user's device may also be collected remotely for the purpose of identification and tracking, using techniques such as the so-called 'device fingerprinting', often without the knowledge of the end-user, and may seriously intrude upon the privacy of these end-users. Techniques that surreptitiously monitor the actions of end-users, for example by tracking their activities online or the location of their terminal equipment, or subvert the operation of the end-users' terminal equipment pose a serious threat to the privacy of end-users. Therefore, any such interference with the end-user's terminal equipment should be allowed only with the	**(20)** Terminal equipment of end-users of electronic communications networks and any information relating to the usage of such terminal equipment, whether in particular is stored in or emitted by such equipment, requested from or processed in order to enable it to connect to another device and or network equipment, are part of the private sphere of the end-users requiring protection under the Charter of Fundamental Rights of the European Union and the European Convention for the Protection of Human Rights and Fundamental Freedoms. Given that such equipment contains or processes information that may reveal details of an individual's emotional, political, social complexities, including the content of communications, pictures, the location of individuals by accessing the device's GPS capabilities, contact lists, and other information already stored in the device, the information related to such equipment requires ~~**enhanced**~~ privacy protection. Furthermore, the so-called spyware~~**, web bugs, hidden identifiers, tracking cookies**~~ and other similar unwanted tracking tools can enter end-user's terminal equipment without their knowledge in order to gain access to information, to store hidden information and to trace the activities ***and may seriously intrude upon the privacy of these end-users***. Information related to the end-user's device may also be collected remotely for the purpose of identification and tracking, using ~~**techniques such as the so called 'device fingerprinting', often without the knowledge of the end-user**~~, ~~**and may seriously intrude upon the privacy of these end-users.**~~ ***web beacons, device identifiers, such as device identifiers, online identifiers, including identifiers stored in so-called cookies, as well as statistical identifiers generated using techniques such as 'device fingerprinting'.*** Techniques that surreptitiously monitor the actions of end-users, for example by tracking their activities

end-user's consent and for specific and transparent purposes.	online or the location of their terminal equipment, or subvert the operation of the end-users' terminal equipment ***without his or her knowledge may*** pose a ~~serious~~ threat to the privacy of end-users. ***At the same time, the same technologies can be used for legitimate and useful purposes such as verifying the identity of users engaged in on-line transactions and understanding the effectiveness of website design and advertising. Where such technologies, for instance cookies, are used for a legitimate purpose, such as to facilitate the provision of information society services, such use should be allowed on condition that it meets the principles of lawfulness, fairness and transparency.*** Therefore, any such ***use*** ~~**interference**~~ with the end-user's terminal equipment should be allowed only with the end-user's consent ***or some other legitimate basis*** and for specific and transparent purposes. ***In line with Regulation (EU) 2016/679, usage of the end-user's terminal equipment should be lawful and fair. It should be transparent to end-users that their terminal equipment's processing or storage capabilities are used or information is collected from their terminal equipment, to what extent and for which purposes. The principle of transparency requires that any information and communication relating to the usage of the end-user's device be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the end-user on the identity of the person responsible, the purposes of the use, and further information as laid down by Regulation (EU) 2016/679.***

This amendment would re-introduce existing language from the current ePrivacy Directive that explains that cookies as a technology do not necessarily serve nefarious purposes but can be used for legitimate purposes, too, such as analytics and advertising purposes and clarifies that the principles of data protection, i.e. lawfulness and fairness, apply in the context of the ePrivacy Regulation.

(21) Exceptions to the obligation to obtain consent to make use of the processing and storage capabilities of terminal equipment or to access information stored in terminal equipment should be limited to situations that involve no, or only very limited, intrusion of privacy. For instance, consent should not be requested for authorizing the technical storage or access which is strictly necessary and proportionate for the legitimate purpose of enabling the use of a specific service explicitly requested by the end-user. This may include the storing of cookies for the duration of a single established session on a website to keep track of the end-user's input when filling in online forms over several pages. Cookies can also be a legitimate and useful tool, for example, in measuring web traffic to a website. Information society providers that engage in configuration checking to provide the service in compliance with the end-user's settings and the mere logging of the fact that the end-user's device is unable to receive content requested by the end-user should not constitute access to such a device or use of the device processing capabilities.	**(21)** Exceptions to the obligation to obtain consent to make use of the processing and storage capabilities of terminal equipment or to access information stored in terminal equipment should be limited to situations that involve no, or only ~~very~~ limited~~,~~ ***impact on the*** ~~**intrusion of**~~ privacy ***of the end-user concerned and in accordance with Regulation (EU) 2016/679. In order to ascertain whether a situation involves no, or only limited, impact on the privacy of the end user concerned, the entity responsible, after having met all the requirements for the lawfulness of using the end-user's terminal equipment, including with respect to transparency, should take into account inter alia: the purpose for which the processing and storage capabilities of the terminal equipment or information accessed are used; the context in which information is collected, in particular the reasonable expectations of end-users based on their relationship with the controller as to the information's further use; the consequences of the intended processing for end-users; and the existence of appropriate safeguards such as encryption or pseudonymisation.*** For instance, ~~**consent should not be requested for authorizing**~~ the technical storage or access which is strictly necessary and proportionate for ~~**the legitimate purpose of**~~ enabling the use of a specific service explicitly requested by the end-user ***may be regarded as carried out for a legitimate interest.*** This may include the storing of cookies for the duration of a single established session on a website to keep track of the end-user's input when filling in online forms over several pages. Cookies can also be a legitimate and useful tool for ***other legitimate purposes,*** for example**,** ***helping to secure a service,*** ~~**in**~~ measuring web traffic to a website ***or delivering and measuring the effectiveness of advertisements.***

	Access to information society services may be made conditional on the well-informed consent to the use of cookies or similar technologies used for legitimate purposes. Information society providers that engage in configuration checking to provide the service in compliance with the end-user's settings and the ~~**mere logging**~~ ***determining*** ~~of the fact~~ that the end-user's device is unable to receive content requested by the end-user should not constitute access to such a device or use of the device processing capabilities.

This amendment would elaborate on the transparency that should be provided to end-users when information stored in and related to their terminal equipment is accessed. It would also re-introduce important clarifications from the existing ePrivacy Directive: Information society services are permitted to make access to their service conditional on consent for the use of cookies and similar technologies.

(22) The methods used for providing information and obtaining end-user's consent should be as user-friendly as possible. Given the ubiquitous use of tracking cookies and other tracking techniques, end-users are increasingly requested to provide consent to store such tracking cookies in their terminal equipment. As a result, end-users are overloaded with requests to provide consent. The use of technical means to provide consent, for example, through transparent and user-friendly settings, may address this problem. Therefore, this Regulation should provide for the possibility to express consent by using the appropriate settings of a browser or other application. The choices made by end-users when establishing its general privacy settings of a browser or other application should be binding on, and enforceable against, any third parties. Web browsers are a type of software application that permits the retrieval and presentation of information on the internet. Other types of applications, such as the ones that permit calling and messaging or provide route guidance, have also the same capabilities. Web browsers mediate much of what occurs between the end-user and the website. From this perspective, they are in a privileged position to play an active role to help the end-user to control the flow of information to and from the terminal equipment. More particularly web browsers may be used as gatekeepers, thus helping end-users to prevent information from their terminal equipment (for example smart phone, tablet or computer) from being accessed or stored.	**(22)** The methods used for providing information and obtaining end-user's consent should be as user-friendly as possible. Given the ubiquitous use of tracking cookies and other tracking techniques, end-users are increasingly requested to provide consent to store such tracking cookies in their terminal equipment. As a result, end-users are overloaded with requests to provide consent. The use of technical means to provide consent, for example, through transparent and user-friendly settings, may address this problem. Therefore, this Regulation should provide for the possibility to express consent by using the appropriate settings of a browser or other application. The choices made by end-users when establishing its general privacy settings of a browser or other application should be binding on, and enforceable against, any ~~**third parties**~~ ***persons other than the end-user concerned***. ***Such general privacy settings should not prevent an information society service from collecting information from or about the end user's terminal equipment with the end-user's consent.*** Web browsers are a type of software application that permits the retrieval and presentation of information on the internet. Other types of applications, such as the ones that permit calling and messaging or provide route guidance, have also the same capabilities. Web browsers mediate much of what occurs between the end-user and the website. From this perspective, they are in a privileged position to play an active role to help the end-user to control the flow of information to and from the terminal equipment. ~~**More particularly web browsers may be used as gatekeepers, thus helping end-users to prevent information from their terminal equipment (for example smart phone, tablet or computer) from being accessed or stored.**~~

This amendment would clarify the intention as expressed by the European Commission that browser settings would not prevent information society services to request specific consent where their general preference is that information is not collected. It would also strike the notion that

browsers and other applications should act as gatekeepers between information society services and their users.

(24) For web browsers to be able to obtain end-users' consent as defined under Regulation (EU) 2016/679, for example, to the storage of third party tracking cookies, they should, among others, require a clear affirmative action from the end-user of terminal equipment to signify his or her freely given, specific informed, and unambiguous agreement to the storage and access of such cookies in and from the terminal equipment. Such action may be considered to be affirmative, for example, if end-users are required to actively select 'accept third party cookies' to confirm their agreement and are given the necessary information to make the choice. To this end, it is necessary to require providers of software enabling access to internet that, at the moment of installation, end-users are informed about the possibility to choose the privacy settings among the various options and ask them to make a choice. Information provided should not dissuade end-users from selecting higher privacy settings and should include relevant information about the risks associated to allowing third party cookies to be stored in the computer, including the compilation of long-term records of individuals' browsing histories and the use of such records to send targeted advertising. Web browsers are encouraged to provide easy ways for end-users to change the privacy settings at any time during use and to allow the user to make exceptions for or to whitelist certain websites or to specify for which websites (third) party cookies are always or never allowed.	**(24)** For ~~**web browsers**~~ **information society services** to be able to obtain end-users' consent as defined under Regulation (EU) 2016/679, for example, to the storage of ~~**third party**~~ tracking cookies, they should, among others, require a clear affirmative action from the end-user of terminal equipment to signify his or her freely given, specific informed, and unambiguous agreement to the storage and access of such cookies in and from the terminal equipment. Such action may be considered to be affirmative, for example, if end-users are required to actively select 'accept third party cookies' to confirm their agreement and are given the necessary information to make the choice. To ***assist end-users in*** ~~**this end, it is necessary to require**~~ ***expressing their privacy preferences*** providers of software enabling access to internet ***may*** ~~**that**~~, at the moment of installation, ~~**end-users are**~~ inform~~**ed**~~ ***end-users*** about the possibility to choose ~~**the**~~ privacy settings among ~~**the**~~ various options and ask them to make a choice. Information provided should not ***unduly*** dissuade end-users from selecting higher privacy settings and should include relevant information about the ~~**risks**~~ ***possible consequences*** associated ~~**to**~~ ***with*** ~~**allowing third party cookies to be stored in the computer**~~ ***that choice***, ~~**including the compilation of long-term records of individuals' browsing histories and the use of such records to send targeted advertising**~~. Web browsers ~~**are encouraged to**~~ ***should*** provide easy ways for ***information society services to ask*** end-users to change the privacy settings at any time during use and to allow the user to make exceptions for or to whitelist certain websites or to specify for which websites ~~**(third) party**~~ cookies are always or never allowed.

In line with the amendments above, this amendment would change the approach from browsers and other applications to intermediate the relationship between information society services and their users. Importantly, it would also clarify that where browsers and other applications provide ways for end-users to express their general preferences they should also make available

functionalities that enable users to make specific choices on a case-by-case basis. If such functionality is merely “encouraged” information society services may effectively lose the ability to request consent from their own users.