Amendments on the ePrivacy Regulation proposed by Mozilla October 2017

ARTICLE 7 - STORAGE AND ERASURE OF ELECTRONIC COMMUNICATIONS DATA		
COMMISSION PROPOSAL	**LIBE DRAFT REPORT**	**MOZILLA PROPOSED AMENDMENTS**
1. Without prejudice to point (b) of Article 6 (1) and points (a) and (b) of Article 6 (3), the provider of the electronic communications service shall erase electronic communications content **or make that data anonymous** after receipt of electronic communication content by the intended recipient or recipients. Such data may be recorded or stored by the end-users or by a **third** party entrusted by them to record, store or otherwise process such data**, in accordance with Regulation (EU) 2016/679**.	1. Without prejudice to point (b) of Article 6 (1) and points (a) and (b) of Article 6 (3), the provider of the electronic communications service shall erase electronic communications content or make that data anonymous after receipt of electronic communication content by the intended recipient or recipients. Such data may be recorded or stored by the **users** or by a **specific other** party entrusted by them to record, store or otherwise process such data, in accordance with Regulation (EU) 2016/679.	1. Without prejudice to point (b) of Article 6 (1) and points (a) and (b) of Article 6 (3), the provider of the electronic communications service shall erase electronic communications content or make that data anonymous **as soon as is reasonable** after receipt of electronic communication content by the intended recipient or recipients. Such data may be recorded or stored by the **users** or by a **specific other** party entrusted by them to record, store or otherwise process such data, in accordance with Regulation (EU) 2016/679.
Justification: We've added further specification to what would constitute "after receipt", to achieve a balance between swift deletion but within a reasonable timeframe. For instance, it is technically possible for IP logs to be deleted immediately after receipt. Retaining these logs for some reasonable amount of time can also be useful for things like fraud detection and analysis.		

ARTICLE 8 - PROTECTION OF INFORMATION STORED IN AND RELATED TO END USERS' TERMINAL EQUIPMENT		
COMMISSION PROPOSAL	**LIBE DRAFT REPORT**	**MOZILLA PROPOSED AMENDMENTS**
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:	1. The use of processing and storage capabilities of terminal equipment and the collection of information from users' terminal equipment, **or making information available through the terminal equipment**, including **information** about **or generated by** its software and hardware, other than by the ~~end-user~~ user concerned shall be prohibited, except on the following grounds:	**1.** The use of processing and storage capabilities of terminal equipment and the collection of information from users' terminal equipment, **or making information available through the terminal equipment**, including **information** about **or generated by** its software and hardware, other than by the ~~end-user~~ 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	(a) it is **strictly technically** necessary for the sole purpose of carrying out the transmission of an electronic communication over an electronic communications network; or	(a) it is necessary for the sole purpose of carrying out the transmission of an electronic communication over an electronic communications network; or ***(aa) it is necessary for the technical quality or effectiveness of a delivered information society service or terminal equipment functionality, and has no or little impact on the privacy of the data***

		subject concerned; or
(b) the end-user has given his or her consent; or	(b) the **user** has given his or her consent; or	(b) the user has given his or her consent ***pursuant to Regulation (EU) 2016/679;*** or
(c) it is necessary for providing an information society service requested by the end-user; or	(c) It is **strictly technically** necessary for providing an information society service requested by the end-user; 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 by the provider of the information society service requested by the end-user.	**(d)** if it is **technically** necessary for web audience measuring **of the information society service requested by the user**, provided that such measurement is carried out by the provider, **or on behalf of the provider, or by an independent web analytics agency acting in the public interest or for scientific purpose; and further provided that no personal data is made accessible to any other party and that such web audience measurement does not adversely affect the fundamental rights of the user;**	**(d)** if it is ~~technically~~ necessary for ~~web~~ audience measurement ~~ing of the information society service requested by the user, provided that such measurement is carried out by the provider, or on behalf of the provider, or by an independent web analytics agency acting in the public interest or for scientific purpose; and further provided that no personal data is made accessible to any other party and~~ provided that such ~~web~~ audience measurement does not adversely affect the fundamental rights of the user;
	(da) if it is necessary for a security update, provided that: (i) security updates are discretely packaged and	(da) if it is necessary for a security ***or product*** updates, ***provided that updates do not in any way undo or weaken***

	do not in any way change the privacy settings chosen by the user; (ii) the user is informed in advance each time an update is being installed; and (iii) the user has the possibility to turn off the automatic installation of these updates; **1a. No user shall be denied access to any information society service or functionality, regardless of whether this service is remunerated or not, on grounds that he or she has not given his or her consent under Article 8(1)(b) to the processing of personal information and/or the use of storage capabilities of his or her terminal equipment that is not necessary for the provision of that service or functionality.**	***~~change~~ the privacy settings chosen by the user.* ~~(ii) the user is informed in advance each time an update is being installed;~~**
2. The collection of information emitted by terminal equipment to enable it to connect to another device and, or to network equipment shall be prohibited, except if:	2. The collection of information emitted by terminal equipment to enable it to connect to another device and, or to network equipment shall be prohibited, except if:	2. The collection of information emitted by terminal equipment to enable it to connect to another device and, or to network equipment shall be prohibited, except if:

(a) it is done exclusively in order to, for the time necessary for, and for the purpose of establishing a connection; or	(a) it is done exclusively in order to, for the time necessary for, and for the **sole** purpose of establishing a connection **requested by the user;** or	(a) it is done exclusively in order to, for the time necessary for, and for the ~~**sole**~~ purpose of establishing a connection **requested by the user;** or
	(aa) the user has been informed and has given consent; or	(aa) the user has been informed and has given consent; ~~or~~
	(ab) the data are anonymised and the risks are adequately mitigated.	(ab) the data are anonymised and the risks are adequately mitigated~~.~~; or
(b) a clear and prominent notice is displayed informing of, at least, the modalities of the collection, its purpose, the person responsible for it and the other information required under Article 13 of Regulation (EU) 2016/679 where personal data are collected, as well as any measure the end-user of the terminal equipment can take to stop or minimise the collection. The collection of such information shall be conditional on the application of appropriate technical and organisational measures	Deleted.	***(ac) if it is necessary for the functioning of the software, where risks are adequately mitigated.***
	2a. For the purpose of point (ab) of paragraph 2, the following controls shall be implemented to mitigate the risks:	**2a. For the purpose of point (ab) of paragraph 2, the following controls shall be implemented to mitigate the risks:**
	(a) the purpose of the data collection from the terminal equipment shall be restricted to mere statistical counting; and	**(a) the purpose of the data collection from the terminal equipment shall be restricted to mere statistical counting; and**
	(b) the tracking shall be limited in time	**(b) the tracking shall be limited in**

to ensure a level of security appropriate to the risks, as set out in Article 32 of Regulation (EU) 2016/679, have been applied.	**and space to the extent strictly necessary for this purpose; and** **(c) the data shall be deleted or anonymised immediately after the purpose is fulfilled; and** **(d) the users shall be given effective opt-out possibilities.**	**time and space to the extent strictly necessary for this purpose; and** **(c) the data shall be deleted or anonymised immediately after the purpose is fulfilled; and** (d) the users shall be given effective opt-out possibilities ***where feasible***.
3. The information to be provided pursuant to point (b) of paragraph 2 may be provided in combination with standardized icons in order to give a meaningful overview of the collection in an easily visible, intelligible and clearly legible manner.	**Deleted**	**Deleted**
4. The Commission shall be empowered to adopt delegated acts in accordance with Article 27 determining the information to be presented by the standardized icon and the procedures for providing standardized icons.	**Deleted**	**Deleted**
Justification: The amendments in ***8(b)*** further clarify the relationship with the GDPR to ensure harmonisation on consent requirements. The addition of the new paragraph ***(ac)***, addresses our concern that the Commission's draft does not allow sufficient flexibility to allow product features to function smoothly, nor enable services to lessen the frequency of consent requests to the end user in the cases of minimal to zero privacy impact. We have stopped short of suggesting that Legitimate		

Interest should be used as a legal grounds for processing. Mozilla's products, such as Firefox, do rely on legitimate interest for a number of non-privacy invasive processing tasks, notably for metrics purposes. We have therefore broadened the exceptions, particularly in ***8(d)*** to create that necessary flexibility to allow the processing of data for smooth software functionality. Furthermore, we strongly encourage looking at guidance from the Article 29 Working Party's Opinion 04/2012 on Cookie Consent Exemption (section 4.3) as well as the French DPA CNIL, which has devised technical guidance providing for an exception for first party analytics. We encourage this approach in the interpretation of the Regulation once it comes into force.

CORRESPONDING RECITALS FOR ARTICLE 8 - (20) & (21)		
COMMISSION PROPOSAL	**LIBE DRAFT REPORT**	**MOZILLA 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,	(20) Terminal equipment of **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 **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 **very sensitive data** that may reveal **details of the behaviour, psychological features,** emotional	(20) Terminal equipment of **users** of electronic communications networks and any personally attributable 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 **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, **unless pseudonymised or anonymised,** ~~very sensitive~~ data that may reveal details of

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	**condition and** political and social **preferences of an individual**, including the content of communications, pictures, the location of individuals by accessing the GPS capabilities **of their device**, contact lists, and other information already stored in the device, the information related to such equipment requires enhanced privacy protection. Information related to the **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 **user**, and may seriously intrude upon the privacy of these **users**. **Furthermore, so-called spyware, web bugs, hidden identifiers and unwanted tracking tools can enter users' terminal equipment without their knowledge in order to gain access to information or to store hidden information.** Techniques that surreptitiously monitor the actions of **users**, for example by tracking their activities online or the location of their terminal equipment, or subvert the	the ~~behaviour, psychological features,~~ emotional condition and political and social preferences of an individual, including the content of communications, pictures, the location of individuals by accessing the GPS capabilities of their device, contact lists, and other information already stored in the device, the information related to such equipment requires ~~enhanced~~ **robust** privacy protection. Information related to the **user's** device may also be collected remotely for the purpose of identification and tracking, using ***mobile advertising identifiers or*** techniques such as the so-called 'device fingerprinting', often without the knowledge of the **user**, and may seriously intrude upon the privacy of these users. **Furthermore, so-called spyware, web bugs, hidden identifiers and unwanted tracking tools can enter users' terminal equipment without their knowledge in order to gain access to information or to store hidden information.** Techniques that ***unlawfully*** ~~surreptitiously~~ monitor the

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 end-user's consent and for specific and transparent purposes.	operation of the **users'** terminal equipment pose a serious threat to the privacy of **users**. Therefore, any such interference with the **user's** terminal equipment should be allowed only with the **user's** consent and for specific and transparent purposes. **Users should receive all relevant information about the intended processing in clear and easily understandable language. Such information should be provided separately from the terms and conditions of the service.**	actions of **users**, for example by tracking their activities online or the location of their terminal equipment, or subvert the operation of the **users'** terminal equipment pose a serious threat to the privacy of **users**. ~~Therefore, any such~~ ***I***nterference with the **user's** terminal equipment should be allowed only with the **user's** consent and for specific and transparent purposes. **Users should receive all relevant information about the intended processing in clear and easily understandable language. Such information should be provided separately from the terms and conditions of the service.**
(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	**(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	**(21)** Exceptions to the obligation to obtain consent to ~~make use of the processing and storage capabilities of terminal equipment~~ ***store information in 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~~ ***comply with ~~all~~ obligations pursuant to Regulation***

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.	necessary and proportionate for the legitimate purpose of enabling the use of a specific service explicitly requested by the **user**. This may include the storing of information (such as cookies and identifiers) for the duration of a single established session on a website to keep track of the **user's** input when filling in online forms over several pages. **Tracking techniques, if implemented with appropriate privacy safeguards**, can also be a legitimate and useful tool, for example, in measuring web traffic to a website. Information society providers **could** engage in configuration checking in **order** to provide the service in compliance with the **user's** settings and the mere logging **revealing** the fact that the user's device is unable to receive content requested by the user, should not constitute illegitimate access.	***(EU) 2016/679,*** **f**or 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 that is beneficial for ~~explicitly requested by~~ the **user**. This may include the storing of information (such as **"**cookies**"** and identifiers), ~~for the duration of a single established session~~ **for example** on a website to keep track of the **user's** input when filling in online forms over several pages. **Tracking techniques, if implemented with appropriate privacy safeguards,** can also be a legitimate and useful tool, for example, in measuring web traffic to a website. ***Similarly, providers of terminal equipment and the software needed to operate such equipment regularly need access to configuration and other device information and the processing and storage capabilities to maintain the equipment, prevent security vulnerabilities and correct problems related to the equipment's operation. Service providers*** **could**

		engage in configuration checking in **order** to provide the service in compliance with the **user's** settings and the mere logging **revealing** the fact that the user's device is unable to recieve content requested by the user, should not constitute illegitimate access.
Justification: These amendments combine the EP Rapporteur and the Commission's draft, providing more clarity and to ensure that the access and processing of device information, which have a very low or no impact on user privacy, such as preventing security vulnerabilities shall be allowed without unnecessarily asking the users' explicit consent.		
ARTICLE 9 - CONSENT		
COMMISSION PROPOSAL	**LIBE DRAFT REPORT**	**MOZILLA PROPOSED AMENDMENTS**
1. The definition of and conditions for consent provide for under Article 4(11) and 7 of Regulation (EU) 2016/679/EU shall apply.	1. The definition of and conditions for consent provide for under Article 4(11) and 7 of Regulation (EU) 2016/679/EU shall apply.	1. The definition of and conditions for consent provide for under Article 4(11) and 7 of Regulation (EU) 2016/679/EU shall apply.
2. Without prejudice to paragraph 1, where technically possible and feasible, for the purposes of point (b) of Article 8(1), consent may be expressed by using the appropriate technical settings of a software application enabling access to the internet.	2. Without prejudice to paragraph 1, where technically possible and feasible, for the purposes of point (b) of Article 8(1), consent may be expressed by using technical **specifications of electronic communications services. When such technical specifications are used by the user, they shall be binding on, and enforceable against, any other party.**	2. Without prejudice to paragraph 1, where technically possible and feasible, for the purposes of point (b) of Article 8(1), consent may be expressed ***or withdrawn by*** using ***~~the appropriate technical specifications settings of a software application enabling access to the internet.~~ which allow for electronic communications services or information***

		society services which allow for specific consent for specific purposes and with regard to specific service providers actively selected by the user in each case, pursuant to paragraph 1. When such technical specifications are used by the user's terminal equipment or the software running on it, they may signal the user's preferences based on previous active selections by him or her.
3. End-users who have consented to the processing of electronic communications data as set out in point (c) of Article 6(2) and points (a) and (b) of Article 6(3) shall be given the possibility to withdraw their consent at any time as set forth under Article 7(3) of Regulation (EU) 2016/679 and be reminded of this possibility at periodic intervals of 6 months, as long as the processing continues.	**3. Users** who have consented to the processing of electronic communications data as set out in point (c) of Article 6(2) and points (a) and (b) of Article 6(3), **point (b) of Article 8(1) and point (aa) of Article 8(2)** shall be given the possibility to withdraw their consent at any time as set forth under Article 7(3) of Regulation (EU) 2016/679 and be reminded of this possibility at periodic intervals of 6 months, as long as the processing continues.	**3. Users** who have consented to the processing of electronic communications data as set out in point (c) of Article 6(2) and points (a) and (b) of Article 6(3), **point (b) of Article 8(1) and point (aa) of Article 8(2)** shall be given the possibility to withdraw their consent at any time as set forth under Article 7(3) of Regulation (EU) 2016/679 ~~and be reminded of this possibility at periodic intervals of 6 months, as long as the processing continues.~~
Justification: We welcome the harmonisation of consent with the GDPR, as well as the codification of user choice to be upheld. We are in favor of the provision supporting technical expression of preferences (often called the DNT provision), and have proposed its inclusion here. As prior participants of the W3C's Tracking Protection Working Group (TPWG, also called the DNT		

Working Group) dialogues, we see this as a helpful advancement to allow browser vendors and other software to effectuate the choices of users. However, one of the primary challenges to DNT's success has been the lack of broad consensus on what it means, though inclusion here has already spurred additional work on DNT standards.

Compliance with DNT will be challenging, even if legally required, when companies do not know what is required to comply and do not have an agreed upon standard to use. Major browsers, including Firefox, have allowed users to turn on a signal called DNT for years. The browser can set a number of signals - such as DNT - but whether or not that signal means anything, or can be complied with by websites is a challenge. We do not believe this current implementation challenge is unsurpassable, but consideration of the technical standards required upon entry into force of the Regulation should be carefully assessed. More guidance, standards, and implementation details will be necessary in order for this provision to work, and these standards continue to be developed at the W3C and elsewhere.

CORRESPONDING RECITALS FOR ARTICLE 9 - (22), (23)		
COMMISSION PROPOSAL	**LIBE DRAFT REPORT**	**MOZILLA PROPOSED AMENDMENTS**
(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	(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, **users** are increasingly requested to provide consent to store such tracking cookies in their terminal equipment. As a result, **users** are overloaded with requests to provide consent. The use of technical means to provide consent, for example, through	(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, **users** are increasingly requested to provide consent to store such tracking cookies in their terminal equipment. As a result, **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	transparent and user-friendly settings, may address this problem. Therefore, this Regulation should **prevent the use of so-called "cookie walls" and "cookie banners" that do not help users to maintain control over their personal information and privacy or become informed about their rights. This Regulation should** provide for the possibility to express consent by **technical specifications, for instance** by using the appropriate settings of a browser or other application. **Those settings should include choices concerning the storage of information on the user's terminal equipment as well as a signal sent by the browser or other application indicating the user's preferences to other parties. The** choices made by **users** when establishing **the** 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	transparent and user-friendly settings, may address this problem. ~~Therefore,~~ **This Regulation should** provide for the possibility to express consent by **technical specifications, for instance** by using the appropriate settings of a browser or other application. **Those settings should include choices concerning the storage of information on the user's terminal equipment as well as a signal sent by the browser or other application indicating the user's preferences to other parties. The** choices made by **users** when establishing **the** 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 advertising and/or the storage and access of data on the user's terminal device, often have*** the same capabilities. Web browsers mediate much of what occurs between the **user**

equipment (for example smart phone, tablet or computer) from being accessed or stored.	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 **user** and the website. From this perspective, they are in a privileged position to play an active role to help the user to control the flow of information to and from the terminal equipment. More particularly, web browsers, **applications or mobile operating systems** may be used as **the executor of a user's choices**, thus helping **users** to prevent information from their terminal equipment (for example smart phone, tablet or computer) from being accessed or stored.	and the website. From this perspective, **they help** the user to control the flow of information to and from the terminal equipment. More particularly, web browsers, **applications or mobile operating systems** may be used as **the executor of a user's choices**, thus helping **users** to prevent information from their terminal equipment (for example smart phone, tablet or computer) from being accessed or stored.
Justification: The Commission's proposal suggests that web browsers are 'gatekeepers' to the internet but there are currently limitations on the ability of browser settings to provide end-users with tools to express consent and enforce privacy requirements on website operators. With affirmative obligations on web browser makers and the large potential penalties for any violation, the Regulation must provide more clarity regarding the privacy features that browser software must provide. Currently, browsers allow users a range of privacy settings which enable them to block all cookies, or only third party cookies and related tracking techniques such as browser and device fingerprinting. Many browsers allow users to send a "Do Not Track" (DNT) request with their browsing traffic, but website operators can ignore or circumvent such requests. The Regulation will specify compliance for DNT and other settings chosen by the end-user, which may alleviate the current issue with cookie		

banners and give more choice, transparency and control to consumers. However it should be noted there is currently no single technical specification(s) that would ensure websites can recognise and comply with these signals. We would appreciate further clarification from the Commission on this point (see our amendments and justification in Article 9 for more details).		
ARTICLE 10 - INFORMATION AND OPTIONS FOR PRIVACY SETTINGS TO BE PROVIDED		
COMMISSION PROPOSAL	**LIBE DRAFT REPORT**	**MOZILLA PROPOSED AMENDMENTS**
2. Upon installation, the software shall inform the end-user about the privacy settings options and, to continue with the installation, require the end-user to consent to a setting.	**Deleted**	2. ~~Upon installation, t~~The software shall inform the end-user data subject about the privacy settings used to prevent third parties from storing or processing information on the terminal equipment. ~~options and, to continue with the installation, require the end-user to consent to a setting.~~
3. In the case of software which has already been installed on 25 May 2018, the requirements under paragraphs 1 and 2 shall be complied with at the time of the first update of the software, but no later than 25 August 2018.	3. In the case of software which has already been installed on 25 May 2018, the requirements under paragraphs 1 and 2 shall be complied with at the time of the first update of the software, but no later than 25 August 2018.	**Deleted**
Justification: These changes strike the right balance to ensure on the one hand, that the user will be presented with a choice, quality privacy service options and clear settings, and on the other, not over-prescribing how and where the user interface should be presented. This allows for more flexible (but meaningfully applied) applications, for e.g. on IoT devices or apps. From Mozilla's view, this would further empower Firefox and other browsers to be the user agent, something that we welcome.		
CORRESPONDING RECITALS FOR ARTICLE 10 - (23) & (24)		
COMMISSION PROPOSAL	**LIBE DRAFT REPORT**	**MOZILLA PROPOSED AMENDMENTS**

(23) The principles of data protection by design and by default were codified under Article 25 of Regulation (EU) 2016/679. Currently, the default settings for cookies are set in most current browsers to 'accept all cookies'. Therefore providers of software enabling the retrieval and presentation of information on the internet should have an obligation to configure the software so that it offers the option to prevent third parties from storing information on the terminal equipment; this is often presented as 'reject third party cookies'. End-users should be offered a set of privacy setting options, ranging from higher (for example, 'never accept cookies') to lower (for example, 'always accept cookies') and intermediate (for example, 'reject third party cookies' or 'only accept first party cookies'). Such privacy settings should be presented in a an easily visible and intelligible manner.	**(23)** The principles of data protection by design and by default were codified under Article 25 of Regulation (EU) 2016/679. Currently, the default settings for cookies are set in most current browsers to 'accept all cookies'. Therefore providers of software enabling the retrieval and presentation of information on the internet should have an obligation to configure the software so that it offers the option to prevent ***by default the cross-domain tracking*** and storing ***of*** information on the terminal equipment ***by other parties***; this is often presented as 'reject third party ***trackers and*** cookies'. Users should be offered, by default, a set of privacy setting options, ranging from higher (for example, 'never accept ***trackers and*** cookies') to lower (for example, 'always accept ***trackers and*** cookies') and intermediate (for example, 'reject ***all trackers and*** cookies ***that are not strictly necessary to provide a service explicitly requested by the user' or 'reject all cross-domain tracking').***	**(23)** The principles of data protection by design and by default were codified under Article 25 of Regulation (EU) 2016/679. Currently, the default settings for cookies are set in most current browsers to 'accept all cookies'. Therefore providers of software enabling the retrieval and presentation of information on the internet should have an obligation to configure the software so that it offers the option to prevent ***the collection of data from the software regarding a particular user's activity across multiple distinct contexts and the retention, use, or sharing of such data derived from that activity outside the context in which it occurred. This includes cross-domain, cross-device, and cross-service tracking*** and storing ***of*** information on the terminal equipment ***by other parties***. This is often presented as 'reject third party ***trackers and*** cookies'. Users should be offered, by default, a set of privacy setting options, ranging from higher (for example, 'never accept ***trackers and*** cookies') to lower (for example, 'always accept ***trackers and*** cookies') and intermediate (for example, 'reject all cross-domain tracking'). These

	These options may also be more fine-grained. Privacy settings should also include options to allow the user to decide for example, whether Flash, JavaScript or similar software can be executed, if a website can collect geo-location data from the user, or if it can access specific hardware such as a webcam or microphone. Such privacy settings should be presented in an easily visible, ***objective*** and intelligible manner.	options may also be more fine-grained. For example, privacy settings could***, where applicable,*** ~~also~~ include options to allow the user to decide for example, whether Flash, JavaScript or similar software can be executed, ~~if a website can collect geo-location data from the user,~~ or if ***software*** can access specific hardware such as a webcam or microphone. Such privacy settings should be presented in an easily visible, ***objective*** and intelligible manner.
(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	**(24)** Deleted	**(24) Deleted**

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.		

Justification: Inspired by the ITRE draft report, we have combined the two recitals into one, ensured technological neutrality, focusing on the harm -- tracking -- instead of only 'cookies'. We've kept the reference to 'cookies' as it may be helpful in providing guidance for future interpretation. We also moved away from explicit and only referencing one software, browsers, thus ensuring the obligations will be applied to other services.

ARTICLE 11 - RESTRICTIONS		
COMMISSION PROPOSAL	**LIBE DRAFT REPORT**	**MOZILLA PROPOSED AMENDMENTS**
1. Union or Member State law may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 5 to 8 where such a restriction respects the essence of the fundamental rights and freedoms and is a necessary, appropriate and proportionate measure in a democratic society to safeguard one or more of the general public interests referred to in Article 23(1)(a) to (e) of Regulation (EU) 2016/679 or a monitoring, inspection or regulatory function connected to the exercise of official authority for such interests.	**(NEW) Article 11a** **1. Union or Member State law to which the provider is subject may restrict by way of a legislative measure the scope of the obligations and principles relating to processing of electronic communications data provided for in Articles 6, 7 and 8 of this Regulation in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22 of Regulation (EU) 2016/679, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary, appropriate and proportionate measure in a democratic society to safeguard one or more of the general public interests**	**11a** 1. Union or Member State **law to which** the **service** provider is subject **in accordance with its main establishment** may restrict by way of a legislative measure the scope of the obligations and principles relating to processing of electronic communications data provided for in Articles 6, 7 and 8 of this Regulation in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22 of Regulation (EU) 2016/679, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary, appropriate and proportionate measure in a democratic society to safeguard one or more of the

	referred to in Article 23(1)(a) to (d) of Regulation (EU) 2016/679.	general public interests referred to in Article 23(1)(a) to (d) of Regulation (EU) 2016/679. ***For requests from a Member State where the service provider is not established, cross-border mechanisms for requests under mutual legal assistance conventions or Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters will be followed.***
	(NEW) Article 11b **1. Union or Member State law may restrict by way of a legislative measure the scope of the rights provided for in Article 5 where such a restriction respects the essence of the fundamental rights and freedoms and is a necessary, appropriate and proportionate measure in a democratic society to safeguard one or more of the following general public interests:** **(a) national security;** **(b) defence;**	**Article 11b** 1. Union or Member State law ***to which the service provider is subject in accordance with its main establishment*** may restrict by way of a legislative measure the scope of the rights provided for in Article 5 where such a restriction is ***strictly limited to specific targets based on reasonable suspicion and pursuant judicial authorisation,*** respects the essence of the fundamental rights and freedoms and is a necessary, appropriate and proportionate measure in a democratic society to safeguard one

	(c) public security; **(d) the prevention, investigation; detection or prosecution of serious criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.**	or more of the following general public interests: (a) national security; (b) defence; (c) public security; (d) the **targeted** prevention, investigation; detection or prosecution of serious criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. ***(NEW) Article 11c*** ***Member States shall not impose any obligation on undertakings that would result in the weakening of the security and encryption of their networks and services.***
2. Providers of electronic communications services shall establish internal procedures for responding to requests for access to end-users' electronic communications data based on a legislative measure adopted pursuant to paragraph 1. They shall provide the competent supervisory	**Deleted**	**Deleted**

authority, on demand, with information about those procedures, the number of requests received, the legal justification invoked and their response.		
Justification: A service is best positioned to properly evaluate whether or not it will comply with a law enforcement request if it has a strong and clear process in place, so we welcome its inclusion and harmonisation in the EU. We've also included several safeguards to ensure targeted, necessary, and proportionate action is taken by LEA in these matters. Existing cross border mechanisms, such as MLATs and EU Investigation Orders have been included and should be utilised. Finally, we've included in 11c a crucial addition to prohibit Member States from imposing any obligations that would result in the weakening of the security and encryption of networks and services.		
CORRESPONDING RECITAL FOR ARTICLE 11 - RECITAL (26)		
COMMISSION PROPOSAL	**LIBE DRAFT REPORT**	**MOZILLA PROPOSED AMENDMENTS**
26) When the processing of electronic communications data by providers of electronic communications services falls within its scope, this Regulation should provide for the possibility for the Union or Member States under specific conditions to restrict by law certain obligations and rights when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard specific public interests, including national security, defence, public security and the	**(26)** When the processing of electronic communications data by providers of electronic communications services falls within its scope, this Regulation **is without prejudice to** the possibility for the Union or Member States under specific conditions to restrict by law certain obligations and rights **set out in this Regulation** when such a restriction **is targeted at persons suspected of having committed a criminal offence** and constitutes a necessary and proportionate measure in a democratic	**(26)** When the processing of electronic communications data by providers of electronic communications services falls within its scope, this Regulation **is without prejudice to** the possibility for the Union or Member States under specific conditions to restrict by law certain obligations and rights **set out in this Regulation** when such a restriction **is targeted at persons suspected of having committed a criminal offence** and constitutes a necessary and proportionate measure in a democratic

prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security and other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, or a monitoring, inspection or regulatory function connected to the exercise of official authority for such interests. Therefore, this Regulation should not affect the ability of Member States to carry out lawful interception of electronic communications or take other measures, if necessary and proportionate to safeguard the public interests mentioned above, in accordance with the Charter of Fundamental Rights of the European Union and the European Convention for the Protection of Human Rights and Fundamental Freedoms, as interpreted by the Court of Justice of the European Union and of the European Court of	society to safeguard specific public interests, including national security, defence, public security and the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. Therefore, this Regulation should not affect the ability of Member States to carry out lawful interception of electronic communications or take other measures, if necessary and proportionate to safeguard the public interests mentioned above, in accordance with the Charter of Fundamental Rights of the European Union and the European Convention for the Protection of Human Rights and Fundamental Freedoms, as interpreted by the Court of Justice of the European Union and of the European Court of Human Rights.	society to safeguard specific public interests, including national security, defence, public security and the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. Therefore, this Regulation should not affect the ability of Member States to carry out lawful interception of electronic communications or take other measures, if necessary and proportionate to safeguard the public interests mentioned above, in accordance with the Charter of Fundamental Rights of the European Union and the European Convention for the Protection of Human Rights and Fundamental Freedoms, as interpreted by the Court of Justice of the European Union and of the European Court of Human Rights. ***Encryption and other technology measures are essential tools to enable secure transactions, communications and storage of communications data while ensuring integrity of the electronic communications infrastructure as a whole. Any measures taken by Member***

Human Rights. Providers of electronic communications services should provide for appropriate procedures to facilitate legitimate requests of competent authorities, where relevant also taking into account the role of the representative designated pursuant to Article 3(3).		***States shall not entail obligations for the provider of the electronic communications network or service that would lead to the weakening of the security and encryption of their networks and/or services.***
Justification: It should be clarified that providers will be responsible for responding to access requests in accordance with the legal requirements of the Member State where the service provider has its principal establishment. Requests for lawful interception of communications across national borders will remain governed by existing mutual assistance arrangements and the European Investigation Order. The obligations of service providers should be clarified with respect to cross-border requests. Furthermore, we recommend following the text used by the ITRE draft opinion that highlights the importance of encryption and the dangers of imposing measures that would result in the weakening of security.		