Mozilla position paper on the European Commission's draft e-Privacy Regulation

The following paper provides an overview of Mozilla's positioning and key recommendations to EU policy makers to support and inform negotiations on the European Commission's proposal for a Regulation on Privacy and Electronic Communications (henceforth ePrivacy Regulation). Our recommendations address the areas of the Regulation which are most closely related to our products and where we could add unique value, including the storage and erasure of data, the protection of information on the terminal device, tracking, privacy settings, and government access to communications and encryption (Articles 7-11).

We look forward to continue working with the Parliament, the Commission, and the Council, by sharing our views and experiences with investing in privacy online. We hope that the Regulation will contribute to a better communications ecosystem, one that offers meaningful control, transparency, and choice to individuals, and helps to rebuild trust online.

TABLE OF CONTENTS

INTRODUCTION

As the European institutions move forward with proposals to reform the EU's electronic privacy framework through the proposal for a Regulation on electronic privacy (ePR), Mozilla would like to contribute to the shared goals of building a healthy internet ecosystem, where user transparency, control, choice are strengthened, and where the confidentiality and security of communications are protected.

The current EU legal instrument regarding electronic privacy, the e-Privacy Directive, is in need of reform. It fails to provide effective privacy protections for users, and yet also imposes inefficient burdens on industry. This dynamic is best illustrated by the "cookie banner," a policy which requires users to click through to "consent" to the use of cookies by a Web site. Not only is the implementation a patchwork of different interpretations of the Directive, but also the banners fail to give users meaningful information about what information is collected, or any ability to effectuate their privacy choices.[1]

Against this backdrop, we welcome the move to update ePrivacy rules to suit the changes of the technological age, to harmonise and strengthen the framework -- with particular attention to coherence with the GDPR -- and to streamline oversight to the data protection authorities.

We also see this ePR proposal as a unique catalyst to help rebuild trust online and bring much needed reforms for user privacy, particularly in the context of advertising. It is our

[1] See, e.g. https://www.theguardian.com/technology/2015/mar/19/cookies-how-to-avoid-being-tracked-online

belief that the current status quo of online advertising is unsustainable. From that perspective, we welcome this process as an opportunity for a broad community of stakeholders to come together and re-evaluate certain practices and their effects -- from ad-fraud, to pervasive tracking, to loss of trust and control of users -- and to move together towards a more sustainable economic ecosystem where user control, transparency, and choice coexist with economic business models.

The following are key aspects of the Commission's draft ePrivacy Regulation that, in Mozilla's view, should be further improved in order to deliver meaningful and effective reforms for users and businesses across the internet ecosystem. We have chosen to comment only on the articles that most directly relate to Mozilla's products, namely the Firefox web browser. It should be understood that we are not endorsing the articles that do not appear in this paper.

We hope these suggestions will ensure that the Regulation endures the test of time, and truly achieves maximal benefits for the privacy and security of communications, with minimum unnecessary or problematic complexities for technology design and engineering.

STORAGE & ERASURE (ARTICLE 7)

Two crucial elements of the privacy of communications are to ensure the data is only stored for as long as necessary, and data which is no longer needed is deleted. For electronic communications, employing anonymisation techniques are likewise important both for the user and for the service; the former because their right to privacy is a fundamental right, and for the service because it greatly reduces the risk associated with collecting and processing communications content and metadata. We thus are generally supportive of this proposal, as it aligns with our data collection processes.[2] However, one area of clarification needed is the threshold for what deletion "after receipt" would require. It is technically possible for IP logs, for example, to be deleted immediately after receipt, but retaining these logs for some reasonable amount of time can also be useful for things like fraud detection and analysis. We would therefore strongly encourage that deletion should follow after a reasonable amount of time and not be required as soon as technically possible.

[2] https://wiki.mozilla.org/Firefox/Data_Collection

RECOMMENDATIONS

- *Mozilla is supportive of the deletion and anonymising obligations, but we invite clarity on what "after receipt" means in practice. Deletion should follow after a reasonable amount of time and not be required as soon as technically possible, to allow useful applications such as fraud detection.*

PROTECTION OF DATA ON TERMINAL DEVICE (ARTICLE 8)

The protection of information stored on a user's device is of utmost importance to trust, control and transparency. The following outlines areas where we see a need to add some flexibility, which in our view, would strike that balance between securing the information on the device, and ensuring the smooth functioning of services.

PROCESSING AND STORAGE

The following are flexibilities we have included which would allow for the use and processing capabilities of the terminal equipment and the collection of information from the user' device in Article 8(1), in addition to consent and the provision of the service:

- ***Necessary for the technical quality or effectiveness of the service:*** this would include processes where it's necessary to access to the communications content itself, such as translators, group video callings, message syncing across devices, or assistive technologies that automatically copy hotel reservations, travel itineraries, and so forth.
- ***Audience measurement:*** for a more technology neutral approach, we suggest removing the "web" qualifier, to ensure that it can apply in various contexts and purposes outside of the narrow scope of web. As an added safeguard, the measurements should not adversely affect the fundamental rights of the user.
- ***Security or product updates:*** This includes scanning, filtering, and ultimately processing both communication content and metadata for the detection and prevention of malware, phishing, and spam, other forms of abuse of networks, services and users in addition to software updates, that are a crucial measure to enhance security. This is providing that updates are discreetly packaged, do not weaken the user's privacy settings, and finally, that the user should have the ability to turn off security updates if they so choose.

CONNECTION TO OTHER DEVICES

We are generally supportive of the rule that collection of information emitted from the user's terminal device to allow it to connect to other devices or network equipment should be prohibited with only limited exceptions in Article 8(2). However, in order to ensure that product features can function properly while still upholding this general rule, we have suggested to include the following. These are in addition to the purposes of establishing a connection by the user, and if the user has been informed and has given consent:

- ***Data are anonymised and risks mitigated:*** mitigating the risks includes limits on data collection to statistical purposes, tracking is limited to what is necessary, the data is anonymised and deleted when connection is achieved, and where possible, users are able to opt out. We have added "where possible" because some processes, particularly those for security, such as DDoS protection, are not possible to opt-out of.
- ***If it's necessary for the functioning of the software:*** The same risk mitigation as per the above shall equally apply.

LEGITIMATE INTEREST

We are concerned the Commission's draft does not allow sufficient flexibility to allow product features to function, and to enable services to lessen the frequency of consent requests to the end user in the cases of minimal to zero privacy impact. Some commenters have suggested that Legitimate Interest could be used as a legal grounds for processing, and indeed it is tempting if we are to consider harmonisation with the GDPR. Furthermore, Mozilla's products, such as Firefox, do rely on legitimate interest for a number of non-privacy invasive processing tasks, notably for metrics purposes (see section above for details). We are concerned however that many companies may make use of the legitimate interest as a loophole to collect and process sensitive data without users' knowledge or control. We therefore would advise against its inclusion.

A frequent justification for Legitimate Interest is to allow for innovation and testing of new products and services. However, we do not believe that the potential risks associated with this broad legal grounds is worth the risk to the privacy of users. Furthermore, it's not necessary for things like product testing and innovation. For Mozilla's part, if we want to conduct research or test browser features that might reveal sensitive information about users, we utilise several experimentation platforms that require users to opt into tests. For

example, users can join the *Test Pilot*[3] program, which will install new addons with additional browser features. Those addons will often provide Mozilla with additional data to understand users' experience with new features. Alternatively, Mozilla also conducts opt-out tests of new features in cases that represent minimal privacy risk to users and where measuring interactions with new features allows us to improve the product for users.

Consistent with our practices and with what we believe to strike an optimal balance, we support broadening exceptions to ensure flexibility for purposes with little to no impact on user privacy, without going as far as to need legitimate interest as a legal grounds for processing in the ePR. We strongly encourage looking at guidance from the Article 29 Working Party's Opinion 04/2012 on Cookie Consent Exemption (section 4.3)[4] as well as the French DPA CNIL, which has devised technical guidance providing for an exception for first party analytics.[5] We encourage this approach in the interpretation of the Regulation once it comes into force.

RECOMMENDATIONS

- *We agree that consent should remain the primary mode for protection metadata, content, and information on the terminal device, but encourage some flexibility to ensure the smooth functioning of product features;*
- *We do not support the inclusion of a broad legitimate interest exception, but we strongly encourage flexibility, by way of broadening the exceptions, particularly for features and functioning with little to no impact on user privacy.*

CONSENT (ARTICLE 9)

We welcome reinforcement of the principles outlined in the GDPR; that relevant settings may be an appropriate way for users to express their choice. We would like to identify some technical challenges in executing such obligations.

[3] https://testpilot.firefox.com/experiments/

[4] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf

[5] https://www.cnil.fr/fr/solutions-pour-la-mesure-daudience

TRACKING

We caution against focusing too heavily on the implementation of one form of tracking (3rd party cookies), as per references in Recitals 22-24, and suggest to focus on the privacy harm this Regulation is seeking to protect against, namely cross-site and device tracking. We support the clear and concise definition[6] crafted by the Tracking Protection Working Group of the W3C, which we offer as a helpful starting point: "*Tracking is the collection of data regarding a particular user's activity across multiple distinct contexts and the retention, use, or sharing of data derived from that activity outside the context in which it occurred. A context is a set of resources that are controlled by the same party or jointly controlled by a set of parties*."

We are concerned that with too much of a focus on one particular implementation of one form of tracking risks driving techniques to more invasive, problematic forms of tracking, such as fingerprinting or mobile advertising identifiers. We are concerned that the Commission's draft focuses too much on regulating behaviour instead of regulating on the basis of principles. The advantage of taking a principled approach is to ensure that the Regulation will stand the test of time, would protect against the range of present and future privacy invasive practices, and apply in various contexts and applications, not only that of the browser and website.

Therefore references to specific tracking techniques should be revised, such as first and third party cookies to ensure that other forms of tracking aren't overlooked. While blocking third party cookies may seem at first glance to be a low hanging fruit to better protect user privacy and security online — see this Firefox add-on called Lightbeam[7], which demonstrates the amount of first and third party sites that can "follow" you online — there are a number of different ways a user can be tracked online; via third party cookies is only an implementation of one form (albeit a common one). Device fingerprinting, for example, creates a unique, persistent identifier that undermines user consent mechanisms and that requires a regulatory solution. Similarly, Advertising identifiers are a pervasive tracking tool on mobile platforms that are currently not addressed. The Regulation should use terminology that more accurately captures the targeted behavior, and not only one possible implementation of tracking.

[6] https://w3c.github.io/dnt/drafts/APIChanges.html
[7] https://www.mozilla.org/en-US/lightbeam/

TECHNICAL EXPRESSION OF PREFERENCES

We are in favor of the provision supporting technical expression of preferences (often called the DNT provision), and have proposed its inclusion in Article 9. 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. 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.

However, we note that the technical compliance specification -- that is, what a server is expected to do if it receives a DNT signal -- has been set aside in favor of outside work. Currently, they are only finishing the specification on signaling. 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.

REMINDERS

On 9(3), we are concerned that for products that do not collect or store user data, the requirement to remind the end user of the possibility to withdraw consent at intervals of 6 months could create a perverse incentive to collect data. This would be counter to the objectives of encouraging anonymisation, minimisation and generally increasing the amount of products on the market that are privacy by default. Furthermore, according to the requirements laid out in the GDPR, controllers and processors of user data will be obliged to offer the right to withdraw consent at any time. We feel this requirement would more appropriately address this issue and would ensure that the user is empowered to effectuate their choices through settings that they can change according to their preferences, but that wouldn't risk unnecessarily over-notifying the user.

RECOMMENDATIONS

- *Focus on the harm -- tracking -- and not the implementation, which will provide more thorough protection for the user and will stand the test of time;*
- *Remove requirement to remind user each 6 months as the user rights which will be introduced by the GDPR will be sufficient.*

PRIVACY SETTINGS (ARTICLE 10)

We view one of the primary objectives of the Regulation to be catalysing more offerings of privacy protective technologies and services for users. We strongly support this objective. This is the approach we have embraced with Firefox: Users can browse in regular mode, which permits Web sites to place cookies, or in private browsing mode, which has our Tracking Protection technology built in. We invest in making sure that both options are desirable user experiences, and the user is free to choose which they go with – and can switch between them at will. We'd like to see more of this in the industry, and welcome the spirit of Article 10 of the draft Regulation which we believe is intended to encourage this. We encourage the Regulation to avoid being overly specific at the level of user interface elements and other technical aspects.

CHOICE

We are generally supportive of the intent of Article 10(2) for web browsers and other services within the scope to make settings more prominent. In Firefox, we're always looking into ways to make these settings more prominently featured and easy to use. However, we caution that from a software developer's' point of view, this provision as written is overly prescriptive in determining when and how to present information about the product to the user, which may conflict with a smooth onboarding process. For instance, in Firefox, we try to minimise the steps the user is taken through to create a swift onboarding process.

10(2) may also be out of step with mobile browsers, IoT applications, and the various other products and services to which this provision will apply. In the worst case scenario it could prompt mass non-compliance, or create a similar situation to what we have now with the so-called cookie banners: prompts are established but they are meaningless, annoying, and don't achieve the purpose of presenting the user with a real choice in how they configure their services. We suggest rather to add a new paragraph specifying that settings should be

easily accessible, and that the software shall inform the end-user about the settings, but not specifying when, how, or what specific information should be provided.

BEYOND BROWSERS

Keeping a principle-based approach will ensure that the Regulation doesn't impose a specific solution that does not meaningfully deliver on transparency, choice, and control outside of the Web browsing context. The draft Regulation includes a particular focus on Web browsers (such as Recitals 22-24), without proper consideration of the diversity of online communications software and platforms today. We aren't suggesting that the Regulation exclude Web browsing, but to focus on one particular client-side software technology risks missing other technology with significant privacy implications, such as tracking facilitated by mobile operating systems or cloud services accessed via mobile apps. Our proposal consequently suggests to delete Recital 24, and we offer modified Recitals 22 and 23 that would provide guidance on the browser example, while acknowledging the application to a range of other services.

RECOMMENDATIONS

- *Reduce the specificity in 10(2) to allow developers to cater their product design and onboarding choices;*
- *Reinforce the importance of presenting the user with clear, easy to understand and easy to use privacy settings;*
- *Keep a principles-based approach, particularly in the recitals, to ensure that the Regulation meaningfully delivers on transparency, choice, and control outside of the Web browsing context.*

SECURITY & ENCRYPTION (ARTICLE 11)

PROCESSES

Mozilla strongly supports regulatory incentives that would require companies to have processes in place to address lawful access requests by state actors. We note that establishing a process by which requests can be fielded can actually benefit companies as without strong, transparent procedures, the risks for greater access to user data may be increased, particularly as increasingly, online service providers are approached by law enforcement and intelligence services to provide access to user data. They are much better off in the case they can demonstrate a clear and accountable process, and are better

empowered to deny those requests if they are overbroad, or do not comply with the process.

The obligation to disclose data to law enforcement authorities in any member state may conflict with company structures which establish the data controlling entity in a particular member state or trigger conflicts of law that impair criminal investigations and put businesses in difficult situations where they may have to comply with incompatible requirements from different jurisdictions. While the ePR suggests that a communications provider established in only one Member State must respond to data access requests from law enforcements from any other 27 Member States, it should be clarified that requests for lawful interception of communications across national borders remain governed by existing mutual assistance arrangements (such as MLATs) and the European investigation Order.

SAFEGUARDS

We encourage the inclusion of procedural safeguards that would ensure at a minimum that any law enforcement request to access users' data is limited to people implicated in the crime; that the data is proportionate and necessary for the investigation in question; and finally, requests are

based on a "reasoned" request backed by a court or independent authority. Authorities should also be obliged to notify users about such requests and companies should be also allowed to do so.

ENCRYPTION

As a preemptive measure, given the concerning trend in the EU and around the world where state actors corrode, undermine, or outright ban critical security measures, strong protections for end-to-end encryption should be included in the ePR. We note that there are currently parallel initiatives being undertaken by DG HOME to explore legal options for law enforcement when accessing electronic evidence. We do not think that such solutions should be carried over into the ePrivacy Regulation.

RECOMMENDATIONS

- *We support the requirement for services within the scope of the Regulation have transparent and accountable processes in place to address lawful access requests by state actors;*

- *We suggest the inclusion of procedural safeguards in 11(2) to comply with the principles of necessity, proportionality, and lawfulness;*
- *We strongly encourage the inclusion (and use of) of existing frameworks such as MLATs and EU systems;*
- *Another layer of protection is needed in Article 11, to prohibit state actors from compelling or coercing services within the scope of the ePR to break, backdoor, or otherwise weaken secure (namely end of end encrypted) communications.*

* * *

For more information, please contact Raegan MacDonald, Senior EU Policy Manager at Mozilla
raegan@mozilla.com

* * *