
webguild

This document contains The Web Guild's responses to the EU's ePrivacy Directive consultation and review.

Date: July 4th 2016

Question 1: Based on your experience, do you consider that the e-Privacy Directive objectives have been achieved? More particularly:

	significantly	moderately	little	not at all	do not know
Full protection of privacy and confidentiality of communications across the EU	○	○	◉	○	○
Free movement of personal data processed in connection with the provision of electronic communication services	○	○	○	○	◉
Free movement of electronic communications equipment and services in the EU	○	○	○	○	◉

Question 1 A: Please specify your reply. You may wish to focus on presenting the reasons why certain objectives were achieved/not achieved, please also consider whether factors other than the e-Privacy Directive influenced the outcome.

Text of 1 to 1500 characters will be accepted

With regards to the cookie policy, objectives have been achieved in as far as there is now more information available on the web from individual websites. But it's not consistently presented, and the public don't read cookie policies.

From our research, of 116 people asked, 52.6% said they find cookie messages "annoying", 44% said they don't take any notice of them, 1.7% said they think they're a good idea but don't read them and 1.7% said they think they're important and usually read the associated privacy policy.

Our own survey of 999 small business websites in the UK revealed that only 26.4% of them included an obvious cookie message. Privacy is of the utmost importance online - but perhaps the "cookie law" doesn't quite achieve the desired result.

Meanwhile the rise in "re-marketing" means that data is increasingly being shared across ad networks / by large web organisations with no regard for the opt in rules around this.

Question 2: Have you encountered problems in applying/understanding the rules (in your role of provider or as individual)? More in particular in relation to:

	Yes	No	No opinion
Notification of personal data breaches	○	○	◉
Confidentiality of electronic communications	○	○	◉
Specific rules on traffic and location data	○	○	◉
Unsolicited marketing communications sent and received though the Internet	◉	○	○
Itemised billing of invoices	○	○	◉
Presentation and restriction of calling and connected line	○	○	◉
Automatic call forwarding	○	○	◉
Directories of subscribers	○	○	◉

Question 2 A: If you answered "Yes", please specify your reply.

Text of 1 to 1500 characters will be accepted

Businesses developing their websites don't understand – or have time to understand – how cookies work and need to be used, so they're relying on their web developer (who isn't a legal professional) to advise them about regulation. Meanwhile, there are often still unknowns around whether the default should be opt-in/opt-out for different kinds of marketing.

Question 3: It is currently up to Member States to set up the national bodies entrusted with the enforcement of the e-Privacy Directive. Article 15a of the e-Privacy Directive refers indeed to the "competent national authority" and, where relevant, "other national bodies" as the entities entrusted with supervisory and enforcement powers in relation to the national provisions implementing the e-Privacy Directive.

On the basis of your experience, did the fact that some Member States have allocated enforcement competence to different authorities lead

	significantly	moderately	little	not at all	do not know
to divergent interpretation of rules in the EU?	○	◉	○	○	○
to non-effective enforcement?	○	◉	○	○	○

Question 4: If you answered 'significantly' or 'moderately' to the previous question, has this in your view represented a source of confusion for:

	Yes	No	Do not know
Providers of electronic communication services, information society services and data controllers in general	◉	○	○
Citizens	◉	○	○
Competent Authorities	○	○	◉

Question 4 A: Please specify your reply.

Text of 1 to 1500 characters will be accepted

In some regards, different interpretations of the rules (cookie messages, the need for consent and questions around assumed consent etc.) do mean websites are playing by different rules – but overall, with so much of the web outside of the EU and so not taking any action in this area, and many sites within the EU still not complying, it's not really member states' position that's causing the confusion and more just a general lack of consistency of having any message at all.

Question 6: Is there an added value to have specific rules for the electronic communications sector on...?:

	Yes	No	No opinion
Notification of personal data breaches	◉	○	○
Confidentiality of electronic communications	◉	○	○
Specific rules on traffic and location data	◉	○	○
Unsolicited marketing communications sent and received though the Internet	◉	○	○
Itemised billing of invoices	○	○	◉
Presentation and restriction of calling and connected line	○	○	◉
Automatic call forwarding	○	○	◉
Directories of subscribers	○	○	◉

Question 6 A: Please specify your reply if needed.

Text of 1 to 1500 characters will be accepted

It's very important to have safeguards in place surrounding privacy online – the problem is that "electronic communications" is a vast subject. It's hard enough to create 1-size-fits-all rules around websites and apps, without then grouping them in with mobile phones or even email.

Question 9: There is legal uncertainty as to whether messages sent through social media are covered by the opt-in provision applying to email (Art 13.1) or by opt-out provisions (Art 13.3). Please indicate whether you agree or not with the following statements.

	Yes	No	No opinion
I find it more reasonable to apply to marketing messages sent through social media the same rules as for email (opt in)	◉	○	○
I find it more reasonable to apply to marketing messages sent through social media opt out rules (Art 13)	○	◉	○

Question 10: The protection of privacy and personal data in the electronic communications sector is also aimed to increase users' trust in these services. **To what extent have the national provisions implementing the e-Privacy Directive contributed to raising users' trust in the protection of their data when using electronic communication services and networks?**

- ○ Significantly
- ○ Moderately
- ◉ Little
- ○ Not at all
- ○ Do not know

Question 10 A: Please specify your reply if needed.

Text of 1 to 1500 characters will be accepted

We're not sure web users feel safer because of this policy... It's probably just highlighted issues that they weren't concerned about before, and in some cases accidentally highlighted non-issues. Cookie messages are often overlooked and not read.

Question 11: To what extent did the e-Privacy Directive create additional costs for businesses?

- ○ Significantly
- ◉ Moderately
- ○ Little
- ○ Not at all
- ○ Do not know

Question 11 A: Please provide an estimation of the percentage of the total cost and/or any other information.

Text of 1 to 1500 characters will be accepted

There were some small costs for website owners to get a developer to add a cookie message - but whilst the costs were very small, they were still a cost a small business didn't want / need. Some small businesses only need to go to their developer once or twice a year for minor updates so this did take up a large percentage of their budget. Meanwhile it's become something extra web developers need to consider on all new websites, without any added value for the client so isn't always something you feel you can cost into a project. (Invariably, as soon as a cookie message / privacy policy is mentioned a client asks their web developer what it needs to say, have they got a sample cookie policy they can copy etc. etc.).

Going forward, when the GDPR comes into force, more costs may be faced as people need to provide more sophisticated online systems to allow users to view, edit, delete, export or even migrate their data. Shop software may also need to be changed to not store details by default, or caveats around data protection and accountancy/recording keeping need to tie in with these privacy rules more coherently.

The directive also talks about websites explaining all the possible risks involved with using it, which often isn't done - but if it was it would cost money in technical consultancy fees.

These are all costs that businesses outside the EU won't face, leaving them with less marketing budget than if they were overseas.

Question 12: In your opinion, are the costs of compliance with the e-Privacy Directive proportionate to the objectives pursued, in particular the confidentiality of communication as a measure to safeguard the fundamental right to privacy?

- (•) Yes
- ( ) No
- ( ) No opinion

Question 12 A: Please specify your reply if needed.

Text of 1 to 1500 characters will be accepted

Adding a cookie message is a small price to pay for privacy... But we don't feel that the cookie messages themselves really add to any increased confidentiality or privacy.

Meanwhile telling someone all about the possible risks with a website is again great in principle but a waste of money if no one reads them. Perhaps details on the risks should be provided – in 1 central location – by the member state. But this could then just result in a long generic document that again no one reads.

Privacy does need to be taken extremely importantly by website owners as they're – intentionally or otherwise – often in a position of holding a lot of data. However a balance needs to be found for small websites compared to large social networks. And any regulations need to be careful about penalising law abiding website owners – with costs and effort – when potentially the websites which do want to get their hands on private information are the ones which may not abide to laws anyway.

Question 13: Do you think that national measures would have been/be needed if there were no EU legislation on e-Privacy for the electronic communication sector?

- (●) Yes
- ( ) No
- ( ) No opinion

Question 14: In your experience, to what extent has the e-Privacy Directive proven to have a clear EU added valueto achieve the following objectives:

	Strongly agree	Agree	Disagree	Strongly disagree	Do not know
Increasing confidentiality of electronic communications in Europe	( )	(●)	( )	( )	( )
Harmonising confidentiality of electronic communications in Europe	( )	(●)	( )	( )	( )
Ensuring free flow of personal data and equipment	( )	( )	( )	( )	(●)

Question 15: Based on your experience with the e-Privacy Directive and taking due account of the content of the GDPR, what should be the priorities for any future legal instrument covering privacy and data protection issues in the electronic communications sector? Multiple answers possible:

- [x] Widening the scope of its provisions to over-the-top service providers (OTTs)
- [x] Amending the provisions on security
- [x] Amending the provisions on confidentiality of communications and of the terminal equipment
- [x] Amending the provisions on unsolicited communications
- [x] Amending the provisions on governance (competent national authorities, cooperation, fines, etc.)
- [ ] Others
- [ ] None of the provisions are needed any longer

Question 17: Should the scope be broadened so that over-the-top service providers (so called "OTTs") offer the same level of protection when they provide communications services such as Voice over IP, instant messaging, emailing over social networks).

- (•) Yes
- ( ) In part
- ( ) Do not know
- ( ) Not at all

Question 18: If you answered "yes" or "In part" to the previous question, please specify which e-Privacy principles & obligations should apply to so called OTTs (multiple replies possible):

	Strongly agree	Agree	Disagree	Strongly disagree	Do not know
Security obligations	◉	○	○	○	○
Confidentiality of communications (prior consent to intercept electronic communications)	◉	○	○	○	○
Traffic and location data (prior consent to process)	◉	○	○	○	○
Unsolicited marketing communications (i.e. should Article 13 apply to messages sent via OTT services?)	◉	○	○	○	○

Question 22: The practice of websites to deny access to those users who refuse to accept cookies (or other technologies) have generated critics that citizens do not have a real choice. **To what extent do you agree to put forward the following measures to improve this situation?**

	strongly agree	agree	disagree	strongly disagree	do not know
Information society services should be required to make available a paying service (without behavioural advertising), as an alternative to the services paid by users' personal information	○	○	○	◉	○
Information service providers should not have the right to prevent access to their non-subscription based services in case users refuse the storing of identifiers in their terminal equipment (i.e., identifiers not necessary for the functioning of the service)	○	○	○	◉	○

webguild

Question 22 A: Please explain, If needed.

Text of 1 to 1500 characters will be accepted

For some services, it would be a lot of work to create a payment platform which they may know that no one would use if it's a relatively low value service. Meanwhile a publisher may feel they need cookies in order for their site to give the user experience they wish to (or add to their reporting in important ways).

If this question relates to ad-blockers, allowing websites to display ads is what powers the free web and allows independent publishers to survive. We would be concerned about freedom of expression and small voices being heard if everyone relied on ad-blockers meaning only large media corporations could afford to run content websites. That's not to say we don't think ad-blockers should exist - but just as an individual has a right to use an ad-blocker if they so wish, a website should have the right to keep their content to themselves if an individual doesn't want to help with the funding of that website by blocking ads.

The expression "banner blindness" is a well heard term in our industry - a lot of web users aren't phased by ads and accept them as the means by which they can get free information. When a banner is intrusive or irritating it's not an ePrivacy issue, it's a bad User Experience issue and should be addressed by the website publisher so as to retain and grow their audience.

Question 23: As a consumer, do you want to be asked for your consent for the processing of your personal data and other information stored on your smart devices as regards the following? Select the option for which you want to be asked for your consent (several options possible):

- [x] Identifiers placed/collected by a third party information society service (not the one that you are visiting) for online behavioural advertising purposes
- [ ] Identifiers placed/collected by an information society service you are visiting – when their purpose is website analytics, measuring number of website visitors, where visitors go within the website, etc. (e.g. "first party" cookies or equivalent technologies)
- [ ] Identifiers placed/collected by an information society service you are visiting whose purpose is to support user experience, such as language preference cookies[1]
- [ ] Identifiers collected/placed by an information society service to detect fraud
- [ ] Identifiers collected/placed by and information society service for frequency capping (number of times a user sees a given ad)
- [ ] Identifiers collected and immediately anonymised in a way that it is impossible to identify the users' device
- [ ] Other

webguild

Question 23 A: Please explain, If needed.

Text of 1 to 1500 characters will be accepted

If someone chooses to visit and to use a website, then they have chosen to use that service in the way it currently operates. It would be good to have a privacy policy available if they chose to see it, but they don't necessarily feel the need to opt in to cookies for that website.

3rd party cookies which share information feel very different. A Facebook "like" button being on a page would mean 3rd party cookies - as long as Facebook didn't track a visitor's presence on the site, but only recorded anything about their interaction with the button, that would be fine as that would be a deliberate choice on the visitor's part. It's when a 3rd party - such as Facebook - tracks a presence on a site so as to show advertisements for the site afterwards, or other sites it thinks someone might like (effectively selling advertising to other companies based on data it's collected about individual user's browsing habits) that privacy feels extremely invaded.

Whilst we don't believe that consent should be required for User Experience features, website publishers should use this freedom wisely and avoid anything that would feel like an invasion of privacy. Websites for example which greet you by name on your return - when you're now logged out - feel over familiar.

Any regulations need to be clear around their stance on session cookies - these may store their existence on a browser/device so debatably fall into the "cookie" category but are often required for a site to function.

Question 24: It has been argued that requesting users' consent to the storage/access of information in their devices, in particular tracking cookies, may disrupt Internet experience. **To facilitate this process and users' ability to consent, a new e-Privacy instrument should (several options possible):**

- [x] Require manufacturers of terminal equipment including operating systems and browsers to place on the market products with privacy by default settings (e.g. third party cookies off by default)
- [ ] Adopt legislation, delegated acts for example, defining mechanisms for expressing user preferences regarding whether they want to be tracked
- [ ] Mandate European Standards Organisations to produce standards (e.g. Do Not Track; Do not Store/Collect)
- [x] Introducing provisions prohibiting specific abusive behaviours, irrespective of user's consent (e.g. unsolicited recording or filming by smart home devices)
- [ ] Support self-co regulation
- [ ] Others

Question 24 A: Please explain, if needed.

Text of 1 to 1500 characters will be accepted

Prohibiting anything is dangerous territory in case you inadvertently stop a legitimate activity. So whilst we have ticked "Introducing provisions prohibiting specific abusive behaviours, irrespective of user's consent" please appreciate this is because of the end of that sentence – "(e.g. unsolicited recording or filming by smart home devices)" and refers to those activities specifically. We are also aware it's important to consider how technology will evolve before these provisions are next reviewed.

We feel more could be done by browsers although enforcing defaults should only be done if a User is aware that defaults have been set. (This is an area our organisation is currently giving more thought to.) Individuals need to take some responsibility for their browsing habits and so any software features should perhaps be flagged up to a user (perhaps periodically) so they can review their decisions.

Websites could also tell Users if they're missing any added value features which they may wish to turn on.

A tricky area is around analytics – if website publishers in the EU aren't able to analyse and understand their user's habits in the way publishers can in the rest of the world then they could be at a severe disadvantage to other companies.

Question 25: The e-Privacy Directive contains specific privacy protections for the processing of traffic and location data in order to ensure confidentiality of the related communications. In particular, they must be erased or made anonymous when they are no longer needed for the purpose of the transmission of a communication or consent to users should be asked in order to use them for added value services (e.g. route guidance, traffic information, weather forecasts and tourist information). Under the existing exemptions, the processing of traffic data is still permitted for a limited time if necessary e.g. for billing purposes. See background document for more details.

Do you consider that the exemptions to consent for processing traffic and location data should be amended? You can choose more than one option. In particular, the exceptions:

- [x] should be broadened to include the use of such data for statistical purposes, with appropriate safeguards
- [x] should be broadened to include the use of such data for public purposes (e.g. research, traffic control, etc.), with appropriate safeguards
- [x] should allow the data to be used for other purposes only if the data is fully anonymised
- [ ] should not be broadened
- [ ] the provision on traffic and location data should be deleted

Question 25 A: Please explain, If needed.

Text of 1 to 1500 characters will be accepted

We're an information age and if we can learn from statistics and create other useful services or information services thanks to gathered data then it feels like a shame to waste this information. Publishers within the EU need to remain competitive against companies from outside who can learn from this sort of data.

However, very often we don't need to know any specifics about a person to help us with generic usage stats. It's very important that anywhere that personal data is being retained it is done so on an opt-in basis, but if it can still be useful once it is completely anonymised then that could be of benefit. A question here though is whether an IP address - or user agent - anything which can just help a website determine an otherwise anonymous user from another otherwise anonymous user (for unique user tracking etc.) counts as "anonymous" or not. The majority of website publishers have no way of tying a persona to a user agent/IP address, but to some ISP/specialist companies this data could be linked to personal details.