SPEECH/11/461

Neelie Kroes

Vice-President of the European Commission responsible for the Digital Agenda

Online privacy – reinforcing trust and confidence

Online Tracking Protection & Browsers Workshop

Brussels, 22 June 2011

Thank you for inviting me to address this workshop on online tracking protection and browsers. It is a pleasure to be amongst so many experts in this field.

I would like to take the opportunity to kick this event off by setting out my vision for online privacy in the digital age.

I will also say a few words about the implementation by EU Member States of the ePrivacy Directive – and about self-regulation and compliance with the new rules in general.

I will conclude by detailing why I believe we need to broaden the discussion and what should be done next – at EU level and beyond.

Privacy in the digital age

Concerns about privacy in the digital age are nothing new. Back in 1999 Scott McNealy of Sun famously said: 'You already have zero privacy – get over it'. Now, I'm sure this was meant partly as a provocative remark, but it reveals an important misconception that many people had even then – that you somehow have to leave your right to privacy at the door when you enter the online world.

Needless to say, I don't agree! In Europe everybody's personal data is protected, offline and online. This becomes more important as the internet turns into a much more social environment. Millions of us share our information, thoughts and photos every day, with friends and others. The very way we interact is changing and brings exciting new opportunities.

But I am also worried by what we see happening: data breaches affecting thousands if not millions; social networking sites rolling out new features with very open default settings; exposure, and identity theft. Privacy is not just about technical features. Without privacy, consumers will not trust the online world. And without trust, the digital economy cannot reach its full potential.

This is not just an abstract statement. One target of the Digital Agenda is to have 50% of Europeans buying online by 2015. We will not reach this without reinforcing trust and confidence.

I said in a recent speech that I have a dream for copyright in the digital age. Well, I have a dream for privacy in the digital age too. I want to see the principles of transparency, fairness and user control running through everything.

Transparency so that citizens know exactly what the deal is. Fairness so that citizens are not forced into sharing their data. And user control so that citizens can decide – in a simple and effective manner – what they allow others to know. Those are key elements of the EU's ongoing review of data protection law, which should lead to a legislative proposal later this year.

The ePrivacy Directive and tracking

But a key part of the EU's legal framework is the ePrivacy Directive, which has already been amended in the latest Telecoms Package. This amendment gives citizens more control over which data is stored or accessed on their digital devices.

For this to become a reality across Europe, timely and correct implementation of the revised provisions by Member States into national law is essential. Unfortunately, so far only five countries – Denmark, Estonia, Finland, Sweden and the United Kingdom – have notified measures to implement the new rules in full. To the other Member States I say that we are prepared to give further guidance should they so wish.

This revision of the ePrivacy Directive has brought a material strengthening of protection for citizens and Member States need to make sure this is reflected in national law. The Commission will use its full powers against Member States that delay.

How to comply

Understandably there is a lot of attention on what this means for web browser cookies. Cookies allow many useful things, for example personalising websites. But they can also be used to track users across different websites. The resulting information can be used to build user profiles which are valuable, for example, for targeting ads.

Some say such tracking is not a problem because targeted ads are more useful for users. Personally, I have a lot of sympathy with that point, but each user should be able to make up their own mind about the value that such advertising represents for them. In addition, once user profiles exist they can potentially be used for all kinds of things. Even after they are no longer of interest to advertisers. The point, therefore, is that users should be able to know, and control, when and to whom they give their information and how it will be used. Hence we need, once again, transparency, fairness and user control.

In a speech last September I set out how industry should react to the new rules in the Directive. I said the way forward is to respect personal preferences and to strike a balance between protecting privacy and enabling business innovation. I addressed advertising specifically because it is an important part of the internet economy.

The role of self-regulation

I confirmed that industry could use self-regulation to achieve compliance. If those doing business online get together and agree on a common way to comply with the law, everybody will benefit: companies will know what they need to do, citizens will quickly learn what to expect and the competent authorities will benefit from simplified enforcement.

Therefore it is encouraging to see that the advertising associations EASA and IAB Europe recently adopted a Best Practice Recommendation and Framework on behavioural advertising. Their approach consists of an icon on each targeted ad, coupled with an information website that allows the user to switch off behaviourally targeted display ads from any participating company. This currently works by setting opt-out cookies and is backed by an enforcement mechanism. I understand work is under way to sign up more companies and to roll this out across the EU. We welcome these efforts and we have stressed the need to involve all stakeholders, including the data protection authorities and the Article 29 Data Protection Working Party.

I hope this will be carried forward by all interested parties in each Member State, with scope for feedback to drive improvements over time. We will assess progress by the end of this year. A further discussion with stakeholders is planned for 2012.

What I like about this solution is that it is active. Industry is not just saying – as some unfortunately still do – that all is fine because users can disable cookies in their web browsers. Instead, a vital section of the online industry has understood that the ePrivacy Directive is addressed to them and requires action.

Broadening the discussion – 'do-not-track'

But tracking can be used for other things apart from targeting ads. Tracking can also be done in other ways than through cookies, for example by using browser add-ons or browser 'fingerprinting'. It follows that while the sectorial self-regulatory scheme I have just described is important, it does not cover all companies, nor all tracking methods, nor all the purposes for which tracking information is used, which need to comply with the ePrivacy Directive. Therefore we need a broader discussion - but that can still be a discussion led by industry to ensure compliance in as business- and consumer-friendly a way as possible. More specifically, I think we should collectively pay more attention to the emerging 'do-not-track' technologies – or DNT for short.

DNT is simple: users can instruct their device or application to accompany all network requests with an indication that they do not want to be tracked. Service providers need to react to such explicit requests.

DNT has a lot of potential because it can apply:

First, to all networked devices and applications

Second, to all types of tracking and

Third, to all purposes of tracking.

DNT is already deployed in some web browsers. And some web businesses say they honour it.

But this is not enough. Citizens need to be sure what exactly companies commit to if they say they honour DNT. For example, there is an important difference between a commitment not to record tracks and a commitment not to use them for a specific purpose once recorded. When this is solved more users will deploy DNT – and it will become simpler – and companies will go along. So we are looking at a virtuous circle.

How do we get there? We need a standard! We need to standardise how the DNT signal and the expected reaction should look. The standard must be rich enough for users to know exactly what compliant companies do with their information and for me to be able to say to industry: if you implement this, then I can assume you comply with your legal obligations under the ePrivacy Directive.

I am sure regulators in other jurisdictions will want to do the same!

The internet is a global achievement and privacy is a global concern. So our technical approach to it must also be global, and fit the generative network.

Fortunately we do not start from scratch. Drafts for a DNT standard already exist. Therefore I am confident that a standardisation initiative for DNT can progress quickly. I am committed to supporting such an initiative and I invite my colleagues in the EU and elsewhere to join me. The US in particular is a most important partner in this and I am grateful that the Federal Trade Commission, which has already shown an interest in DNT, is represented here today at Commissioner's level. Indeed, I had a chance to discuss this with Commissioner Brill just before my speech. This event therefore is a good occasion to get going in earnest.

I urge all interested parties to come to the standardisation table. And I challenge you to agree a DNT standard by June 2012.

And, while I am on the subject, one group I would especially like to see taking part in this is the online advertising industry – because of its experience and because the self-regulation, which is currently based on cookie technology, will need to address DNT as well.

Conclusion

To sum up: online privacy is at the heart of the Digital Agenda. And this is a big year for EU online privacy, with Member States implementing the ePrivacy Directive into national legislation and the data protection review.

We all stand to lose from fragmented rules, disruption of the internet experience and a lack of trust. Therefore we need a uniform approach to the law and solutions that reinforce our principles of transparency, fairness and user control. If I don't see a speedy and satisfactory development I will not hesitate to employ all available means to ensure our citizens' right to privacy.

Self-regulatory efforts are clearly part of the equation on the implementation side. But we need to go further and look beyond cookies and specific sectors. DNT can help us do this.

I wish you a successful workshop and look forward to the results. Thank you.