24 October 2017
jen@defenddigitalme.com

Dear Mr Dalton,

You have the power this week to influence making the Internet better or worse for young people at the forefront of today's information society. I hope you will choose to make things better.

I am interested in understanding your concerns, ahead of Thursday's e-Privacy Regulation debate and would like to pick up this article, ECR Group to force vote on controversial new ePrivacy rules.

"Consumers regularly use free online services and apps and freely give their data. So long as their privacy and data is protected, which it is under both existing rules and the upcoming data protection laws, we should not remove the incentive for businesses to produce free content."

In summary

1. The Regulation suggests manufacturers make practices safer and more transparent. It does not remove the incentive to produce content which they trade in return for users' personal data, unless you believe such an incentive only exists, and is acceptable, if users don't know they are being used.
2. Children generally do *not* give their data *freely* for third party uses, such as reselling and re-purposing, but rather usually give it expecting it is to be used for one thing, the access to the site or product or app, without an understanding of law and limitations, or a way to enforce them. Apps required in schools for example, or bait-and-switch first free/then pay-for apps, often mean data protection offers little in practice. Where rights cannot be understood or enforced by vulnerable or uninformed users, we need respect for rights to be built-in-by-design at the back end of the technology, and in company practices.
3. EU Kids Online's research shows children are now going online at a younger and younger age, they use devices such as mobile phones and toys more than what adults consider computers, and young children's *"lack of technical, critical and social skills may pose [a greater] risk*[1]*.*
4. Children's privacy and data are often *not* protected, but are exploited by design. Recent analysis regarding privacy disclosure and information collection and sharing practices within children's apps, carried out by the Federal Trade Commission in the US, found that of the 400 children's apps they surveyed *"nearly 60% (235) of the apps reviewed transmitted device ID to the developer or, more commonly, an advertising network, analytics company, or other third party and only 20% of privacy policies disclosed this. "22% (88) of the apps reviewed contained links to social networking services, while only 9% (36) disclosed such linkage prior to download"*.[2]
5. These secret data extractions and transfers to social media third parties, means children lose their autonomy and decision making of who knows what about them, and how that information about them shapes their online experience, such as the adverts they see, is hidden to them. IMCO (on which you sit) and the current Council text suggest deleting Article 17 of the proposal, reducing protections still further.
6. The e-Privacy Regulation in fact considers how technology works more than data protection law does, and how it can harm us in ways that we do not see, like the technological machinery of meta data profiling and price discrimination. It protects the right to freedom of communication, and data held on a device. For example, the confidentiality of the content of communications, stored or accessed on an individual's device — for children this includes toys — the GDPR does not specifically cover this.
7. Children need the additional security and protections of the e-Privacy Regulation to thrive in a digital future. In developed countries, 94% of young people aged 15-24 use the Internet. Their protections, participation and privacy must be made priorities, if the Internet is to be a safe long term vehicle for collaboration, commerce, knowledge, learning, play, and promotion of democracy. It is vital to promote a safe and transparent infrastructure of the Internet of the future, for the benefit of all.
8. We need the e-Privacy Regulation to be forward looking, to be able to inspire good practice, and to encourage change of design by default, to keep up with the level of technological risk.[3]

---

[1] Livingstone et al, 2011, p. 3 http://eprints.lse.ac.uk/52630/1/Zero_to_eight.pdf

[2] Mohapatra & Hasty 2012, p.20 (ibid) http://eprints.lse.ac.uk/52630/1/Zero_to_eight.pdf

[3] #Watchout report https://www.forbrukerradet.no/side/significant-security-flaws-in-smartwatches-for-children/

Children are exploited online without understanding how their data are used

Taking the UN Convention on the Rights of the Child as a starting point for evidence-based policy regarding children's rights in the digital age, there must be a balance to participation (getting access to content) and privacy (protecting of the digital and offline self). It is balance between risk and opportunity. These risks include physical tracking, nudging behaviour, and price discrimination.

EU Kids Online's research shows children are now going online at a younger and younger age, they use devices such as mobile phones more than desktops or what adults consider computers, and young children's *"lack of technical, critical and social skills may pose [a greater] risk.*[4]*"*

Commercial companies exploit the vulnerability this imbalance of power creates.

You only need look at the 2016-17 hacks of edTech company Edmodo, V-Tech, or CloudPets, to see vast data sharing without adequate protections, go wrong.

We are discriminated against by price while buying online, because companies use cookies to track our online habits, locations and preferences. Children need to be able to understand and control the use of their data to have control in their lives. Today companies nudge our behaviours unseen, and children can be particularly susceptible to that. It is unethical for companies to hide it.

Picking up your statement, please also consider that young people are at the forefront of today's information society: 830 million young people representing more than 80 per cent of the youth population in 104 countries are online. Children generally do *not* give their data *freely* for third party uses, such as reselling and re-purposing, but rather usually give it expecting it is to be used for one thing, the access to the site or product or app, without an understanding of law and limitations.

Must free content or automatic access to personal data mean hidden harms?

The Regulation does not remove the incentive for businesses to produce content which they trade in return for users' personal data (or some would call "free"), unless you believe that incentive only exists if users don't know they are being used. The e-Privacy Regulation requires those hidden trade-offs using personal data and data about content and locations, should not be secret. It should be welcomed if it reduces the misuse of children's personal data by app providers and careless third parties behind the scenes, which children cannot see and are actively hidden today.

Far from disadvantaging or diluting the product offering to children, it should ensure data privacy is integral to the health and safety thinking of products (including web sites which are often an information product after all), and known flaws should not be accepted because, "Well, everyone uses lead in their paint, and children want to play with the toys". Harmful digital flaws are a health and safety risk to online activity, and should made unacceptable by design. Strive for safer.

Take only one recent example, consider the findings in Watchout[5], the Internet connected Smart Watches report published this week. John Lewis has immediately acted to remove these unsafe products. Few knew that these watches gathered so make personal data in unsafe ways, were easily hacked, or made profiling and tracking children part of their core business model.
The e-Privacy Regulation creates a need to better acknowledge — and therefore likely improve understanding — how profiling and tracking are used as part of a product and how data are stored on a device. Today the onus is put on the user to know how they are being used, often as-if-by-magic. Uses that are behind the scenes by data brokers and those selling web-marketing behind the scenes are hidden by design.

---

[4] Livingstone et al, 2011, p. 3 http://eprints.lse.ac.uk/52630/1/Zero_to_eight.pdf

[5] #WatchOut Analysis of smartwatches for children https://fil.forbrukerradet.no/wp-content/uploads/2017/10/watchout-rapport-october-2017.pdf

Hackable devices that expose users to a man-in-the-middle-attack can mislead where a child is, and since some parents use these devices to maintain physical security, it is a fundamental flaw.

Communications between a child and an online connected product manufacturer, I would hope you would agree should not be secret. But yet again, this is what many "smart" toys do by design. Shockingly, IMCO (on which you sit) and the current Council text suggest deleting Article 17 of the proposal, reducing protections still further.

Transcripts of every voice recording made by dolls[6], robots and gadgets, may include adults' conversations as the toy cannot know the difference, and these are sent currently to Mattel and similar manufacturers, and often have known hacking vulnerabilities. How happy would you be to know your confidential conversations could be picked up via a plaything in the room? It may be perfectly legal, but the communications of biometrics is in desperate need of better practice. We are far off understanding how machine learning and AI are shaping our children's online world.

Manufacturers are slow to react when researchers discover flaws, and supermarket chains in the UK are still stocking these unsafe items or do not respond to requests. Our UK Ministers have so far ignored our calls to step up and understand how these technologies really work, and can do.

We need the e-Privacy Regulation to be forward looking, to be able to enforce good practice, and to encourage change of design by default if we are to keep up with the level of technological risk.

The e-Privacy Regulation considers how technology works more than data protection law, and how it harms us in ways such as meta data profiling and price discrimination that we do not see. That is where children have strong needs for stronger protections, to protect them as future adults.

Providers of any electronic communication service will be required under the Regulation to secure all communications through best available techniques. It will better regulate unsolicited spam, and support the safety of young people using mail, Skype, Messenger, and other tools. It complements the GDPR and clarifies some of the details, helping manufacturers have more consistent practice.

Current Government Data Policy and Practice in England and Education

You may also consider current UK government data policy on children, and question whether putting commercial benefits ahead of children's rights to confidentiality is the kind of future you think sustainable for good business models, or right for our children's digital integrity and security. If you assert that the e-Privacy Regulation, which is aimed at improving he balance of rights and privacy, should be watered down, you by default accept bad practice should come before child rights to privacy and protection, or think the tech expertise the Regulation has this balance wrong.

You state in the article comment, "*their privacy and data is protected, which it is under both existing rules and the upcoming data protection laws*". Be aware that the Data Protection Act does *not* offer children in the UK any way to object to this practice currently, and GDPR is unlikely to change this.

This is an example of practice we want changed. It is government policy, and an example where policy and legal practice are widely adrift from the accepted public's reasonable expectations. Data Protection law does not offer children all the protection it should. We would welcome action here.

The Department for Education gives 23 million children's individual-level identifiable (not anonymised) personal confidential data to third parties, including journalists and companies without any follow up audit process, without any verification of secure settings the newspaper or office, and we know of proven data retention beyond due dates from our Freedom of Information requests.[7]

---

[6] Hello Barbie https://www.technewsworld.com/story/82842.html

[7] The Telegraph background detail FOI https://www.whatdotheyknow.com/request/pupil_data_sensitive_data_releas

This DfE email was written to confirm the newspaper's "cast iron assurances" that no child would be identified, meaning they would not *publish* identifying data in news stories, but not that they *could* not. The data they were given was identifying and highly sensitive.[8] The Department is outsourcing children's privacy to a vast range of third parties, including companies [The Telegraph], [BBC Newsnight], [The Times] [Private Tutor company Tutor Hunt], [Data consultancies].

We know parents find this government policy shocking, and it is a myth that children do not care about their privacy[9]. We have not yet raised its public profile greatly but are minded to do so as we agree that ePrivacy needs wide involvement and informed debate. We'll certainly need to if we find the Regulation and GDPR do not bring better child protections. We have been discretely trying to fix these policies and weak practices with the Department for Education directly, since 2015. If your interest in e-Privacy extends to the UK as well as the EU Regulation, we would welcome support.

The range of ways in which children are profiled in school-wide applications using children's personal data from school records, often including photographs as well as sensitive personal data, and without consent, are not transparent to pupils and parents, or often even to school staff themselves. The spirit of GDPR recital 38 is that "children merit specific protections" and there is a right to object to automated profiling which "should not concern a child" (recital 71). However these are unlikely to make much difference in schools where the public authority can require the system use and there is a significant imbalance of understanding. The e-Privacy Regulation means clearer consistency of expectations, and system-workings should be made more visible.

Schools in the UK use commercial apps using children's personal data to create hidden profiles

- that create persistent and permanent behavioural records,
- that claim to use AI and machine learning to profile that behaviour and to identify how pupils influence each other in the classroom, using AI to automatically generate seating plans.
- for certain basic functions such as homework communications and tracking, or medical records field-trip management and sickness tracking, and cashless payment systems that store the parents' financial details as well as child's personal profile.
- For biometric profiles of library, print, locker and canteen service use based on fingerprints, that store children's biometric data and children's activity down to the nth degree, even down to what they buy and its nutritional content. Biometrics in schools also use RFID and eye scanning.

The protections of these communications in transit, and how organisations use the data, are vital.

Debate on the reality of child data exploitation and privacy is needed

We would welcome greater public debate and opportunity to ensure the public, parents and pupils understand exactly how children's data are exploited by national government, as well as companies, and apps in the e-Privacy debate. It is high time that the issue of Internet commercial economic benefits, put ahead of the confidentiality of children until now, is publicly understood.

I would be delighted, given your interest in e-Privacy, to discuss ways in which we can raise the profile of the data privacy debate in the UK and where these gaps in digital policy must be addressed. Especially on how using the state education data, and in the growth of edTech, offers children benefits, but must not come at the cost of their exploitation. The experience and insights that those involved in shaping the e-Privacy Regulation, formed over years of careful examination of these issues, brings great value to the table. We certainly need that informed debate in the UK.

If you decide the e-Privacy Regulation is something you wish to undermine, then let's have that public debate in England why, given that everyone with common sense wants a safer Internet for children and one that works for all. In England that safety debate is often championed by Children's

---

[8] See p19 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/472700/NPD_user_guide.pdf

[9] Royal Academy of Engineering http://www.raeng.org.uk/news/news-releases/2010/October/privacy-and-prejudice

Commissioner Anne Longfield whom I copy, with the rest of the European and Reformists MEPs.
I ask for all of your support on behalf of children whom the e-Privacy Regulation will better protect.

Before watering down protections that the e-Privacy Regulation offers, please consider the need to protect vulnerable individuals and children whose personal data "merit special protections" under GDPR (Recital 38), and coming UK Data Protection law. That will require that every use of their data is considered with privacy-by-design and data protection by default (GDPR Article 25), and e-Privacy Regulation ensures that consistency across platforms and purposes. It increases opportunity for the user to gain greater digital understanding. Everyone will surely welcome that.

Some of the common myths about the Regulation have become fears, including that the e-Privacy Regulation is bad for business. These can be dispelled if better understood. I encourage those who have not already, to read the Frequently Asked Questions from EDRI. https://edri.org/epd-faq/

If digital identity is exposed and made insecure; then e-banking, e-commerce and even government that uses our online identity are under threat. That is a real threat to future profit and practice of all, including the press, and all of our common good, economic and otherwise.

As the UK Information Commissioner Elizabeth Denham said recently, privacy is not a threat to innovation. However we know that poor practice and damaged consumer trust do harm.

Privacy will become a positive differentiator for better business and better profit.

Fundamentally you need to ask what kind of environment do you want the Internet to be? This regulation will influence whether it is acceptable for companies' with exploitative practices to lurk in the hidden corners of privacy policies. You accept that they will prey on those who don't understand how 'free' content exploits their digital identity, follows them around every website, profiles their activity and nudges their behaviour in secret. Or you can promote an environment which is open and transparent and offers people protection by default, and active control to choose how they interact with companies. Business will thrive in both. But will our children?

Far from destroying the Internet or being bad for business, the e-Privacy Regulation is vital today, if you want to preserve the safe use, users and infrastructure of the Internet for the future. Not only that the personal data a phone collects and transmits are safe and transparent (data protection), but the hidden mechanics of how and why it does and how manufacturers use it, must improve.

Those lobbying to weaken the e-Privacy Regulation may have short term business fears, but their own long-term good, that of business and the economy depend on good policy and practice.

The e-Privacy Regulation will help deliver that, and offer children better protections.
Please give it your support.

Sincerely,

Jen Persson
Director, defenddigitalme
jen@defenddigitalme.com
m: 07510 889833

By email to: daniel@danieldaltonmep.co.uk
cc: MEPs in the ECR Group and Anne Longfield, Children's Commissioner

---

About defenddigitalme

defenddigitalme is a non-partisan civil liberties group founded in 2015. We campaign for better data privacy in the safe, fair and transparent collection, processing and use of children's data across education in England, with a focus on the policy and practice of the Department for Education National Pupil Database. Jen is an independent member of the Department for Education National Pupil Database Steering Group, and currently involved in advocacy with government, educational organisations, industry, and child rights organisations, as we prepare for GDPR, and growth of edTech. For more, see: http://defenddigitalme.com/