

Silent Spring

What if the GDPR was real ?



John Looney

Hello everybody! Thank you for coming to SRECon and giving up your time to listen to me.

This talk will be a little less technical, but hopefully still as fascinating and thought provoking as the week's other talks.

We are going to think about... What if the gdpr was REAL!



Hello!

I'm John Looney

I've been in many large tech companies, that all happened to store personal information.

2

I'll introduce myself properly... I'm John looney, I've been part of SRECon many times, though my career seems to get further away from SRE proper over time. I'm a kind of full-stack engineer; I happy to go from transistors to load balancers, from data center automation to middle management. This has led me to take a very wide view of our industry, and one thing that's concerned me a lot over the last decade is how it feels impossible to square modern privacy legislation with how our industry builds software today.

I have to apologise. This talk was supposed to be a double act, with Simon McGarr, who has thought more about data privacy than everyone in this room put together. But having a wonderful legal mind does not mean one is an expert at calendaring; instead you will have to settle for his inspiration and my execution.

We had spent a lot of time recently , thinking about what would happen if we had an efficient legal system, that could apply the letter of the law to all companies that stored people's data.

I'm not a lawyer, so ... take legal advice before acting on anything we discuss today.

1

Seven Years Ago

I sat up here and chatted about Data Privacy with a Lawyer, and it scared some SREs

3

The best talks are by people who can tell you the future. It's why people loved Ted Talks back when they were good. They seemed prophetic. Seven years ago, I interviewed Simon McGarr, to wrap up the second emea SREcon. He made some bold predictions about various privacy-impacting legal challenges, and their repercussions.

If you'd like to check out the recording, it's still on the USENIX website. For those who don't remember, I will recap....

// Recap on what was [said seven years ago](#) [2 mins]

*"We've challenged the
independence of the Data
Protection Commissioner"*



Simon mentioned that the Irish DPC didn't seem independent ([222s](#)). Since then....

- European Parliament has demanded the European Commission sue Ireland for of the DPC's failure to act promptly at the EU's highest Court
- Two new data protection commissioners were appointed, to ensure at least one of them was a legal expert
- The EU Committee on Civil Liberties visited Ireland - to express concern over the slow pace of regulation, especially taking two years to investigate tiktok's practices, without any action.

"The Safe Harbour is basically a bunch of letters of reassurance"



Simon mentioned that Safe Harbour wasn't really a law, just a pinky-promise. It has been since struck down as not being adequate, leaving any company that relied it to transfer data out of the US without a legal basis for doing so. ([382s](#))

*"If one entity lives in the USA, it's
susceptible to all US law"*



We suspected that Privacy Shield ([1015s](#)), its replacement, wasn't legal either, because it didn't matter if a US company signed a contract saying they would protect EU citizens personal data.

They would still have to provide it, without oversight or redress, to any US government department that was allowed to access it.



The EU Parliament considered Privacy Shield insufficient back in 2016, but it took until 2020 to get that confirmed in court.

In response, we got a brand new fellow in a top hat and a fine mustache. The US-EU Privacy Framework! They ran out of catchy names

"If you suspected the NSA collected data on you, which independent body would you complain to ?"

"Yes. There are difficulties".



We mentioned the lack of an Independent Data Protection Authority, for complaints about US government overreach ([682s](#))

- The Privacy Shield Ombudsperson from the US Gov didn't meet the standards of Independence required.
- So now, the EU have a Civil Liberties Protection Officer. They are also an intelligence officer, and may not be as impartial as we would like when investigating overreach by security services.
- Europeans can now appeal to a Data Protection Review Court (which isn't a court).

"The UK is now a third party country, no benefit of presumed adequacy...I see the investigatory powers act being a problem..."



We also talked about how Brexit might throw up interesting issues. Few thought Teresa May or Boris Johnson would have much interest in regulatory alignment with the EU on data protection.

Would the UK diverge from the EU legal framework with its 'investigatory powers law' ([1959s](#)) ? That was the one Teresa May was responsible for, before becoming PM.

In August 2023, The UK Court of Appeal upheld Liberty's argument that the regime for sharing material from bulk personal datasets with overseas states was unlawful.

- Who will be the UK version Schrems be? Any volunteers ?

2

What's Happening?

The EU legal landscape is getting VERY interesting

10

OK, so. We knew there would be some interesting decisions made over the last few years, and they came about as predicted.

In general, the one thing we were wrong about was how long it took for various things to happen.

Rather than two or three years for Safe Harbour to fall, it took seven.

However, the GDPR is only one law that impacts the tech industry. Let's take a look at some other ones that you may not have been made aware of....



Data Rights Expansion

Collective Redress

2020/11/25

- Like 'Class Action'
- Qualified Entities

Digital Services Act

2022/10/20

- Moderation transparency
- Recommendations transparency
- No 'Dark Patterns'

You don't need to read all this, look it up on Wikipedia later.

- Collective Redress intends to make it easier for consumers to take mass-action against companies that have wronged them. It's class action...with European characteristics. The EU don't like the US approach, where most money seems to be collected by lawyers, and anyone can take any madcap complaints against companies
- Instead, we will have "Qualified Entities", who can be trusted by the courts to sort through the mad claims from sensible ones, and take a modest fee. They will be nominated by national governments. None are named yet.
- If you think this is exciting...good news! You may be one of the 530m people whose data was leaked by Facebook in 2021. You can go to the digital rights Ireland website, and sign up to join that mass action today. It's free, and a fun opportunity to exercise your legal right to redress!
- The Digital Services act made explicit that moderation and recommendation decisions - especially those driven by machine learning - need to be transparent. This extends the GDPR idea that decisions that impact you materially must be explainable to the user, and to a court. How many of your employers ML use-cases could you would struggle explain to a non-technical judge?
- It has provisions that bans 'dark patterns'; practices that try to distort or impair,

- the ability of recipients of a service to make autonomous and informed choices or decisions.
- Platform operators can be held accountable for misinformation from user generated content for the first time...with fines of up to 6% of turnover mentioned.



Consumers Take Back Control

Digital Markets

2024/03/04

- 45m+ users
- Network Effect

ePrivacy

Mid 2024

- E2E encryption
- All message data
- consent > software

Data Act

Mid 2025

- Data portability
- Right to Access
- Organization firewalls

13

Like the GDPR, all of these will be Regulations, that become EU law, and don't need to be transposed into national laws

- The Digital Markets Act takes aim at the network effect that made the second generation of social media companies so dominant. It's based on the same legal theory that inspired the "Quadratic Voting" that Europeans use to elect their MEPs. A country four times as large should only have twice as much say in Parliament. This explicitly values the voice of smaller nations. With the DMA, it will explicitly favour smaller companies, by adding more regulations, the larger companies get.
- It will require federation, portable social network data exports, etc. But it's not just social media - it's targeted at operating systems, browsers etc. - anywhere that a network effect has generated a dominant player. It has been criticised as reducing innovation..like all pro-competiton law.
- The ePrivacy Regulation replaces the old ePrivacy directive, with stronger rules around end to end encryption, and what companies - and governments - can do with Metadata (as well as other non-personal data). It formalises court rulings that felt blanket metadata collection for intelligence or law enforcement is disproportionate.
- One interesting wording in the last draft of the ePrivacy directive, makes it explicit that bugs or missing features - which make it hard to withdraw consent for previously agreed use of data - are a legal liability. You have to expose a

- method to change those agreements...not just a blanket OK when you start an app.
- Oh. The silly cookie warnings are going away. Only needed for privacy-violating ones in future.
- The Data Act is still in its early stages. but it's seen as requiring user-data sharing & interoperability by all companies. It has been roundly criticised by companies as likely to be expensive, difficult, and impacting innovation. As well as mandating data-portability between services (like training data, for a virtual assistant), it also forbids Gatekeeper services like Amazon from using your purchase history with third-party resellers - they must implement internal data firewalls.
- Interestingly for SREs, portability between cloud services is to be mandated -cloud providers should use open standards where possible to facilitate this. I can imagine those of you who are cloud customers are smiling, while those of you working for cloud companies are wondering how they heck you can build an IAM role importer that can read one of your competitors backups. Or how you can import a DynamoDB database into Elasticsearch. I'm not sure the law cares about the nuance of database engine architecture. They just mandate that it has to be portable.



Empowering Consumers

- Collective Redress
- Digital Services Act
- Digital Markets Act
- Data Act
- ePrivacy Regulation

Taken together, this set of acts from the EU are likely to act in concert with the already significant impact of the EU's GDPR to provide consumers with a huge boost in both rights and the means by which to enforce them.

These new laws each have the potential to be as impactful as the GDPR. And all five will seem to land around the same time. The legal version of a five-knuckle sandwich, as it were.

It certainly feels that the way the internet currently works is not compatible with these laws intended to protect citizens. This has happened before.

3

Silent Spring

Let's imagine what would happen to today's world, if all of these new laws were applied

The talk was named after Rachel Carson's Silent Spring, where she imagined what would happen if the world kept using pesticides as it had been using them into the 1960s. Sometimes it can be hard to imagine the future, without a lot of specific examples.

I'm sure in the 1960s, many people assumed that without the blanket use of DDT, that the human race would starve. We didn't.

Europe has chosen a 'rights based' approach to privacy. It starts with the assumption that everyone has the right to a private life, with control of personal data about them. This is considered more important than other people's right to a business model, or law enforcement's duty to protect people from nebulous threats that may be detected by broad and novel uses of personal data.

These laws were written by people with memories of the Stasi, who knew what happens when data is collected through many different sources, then made available to government departments and other nefarious organisations.

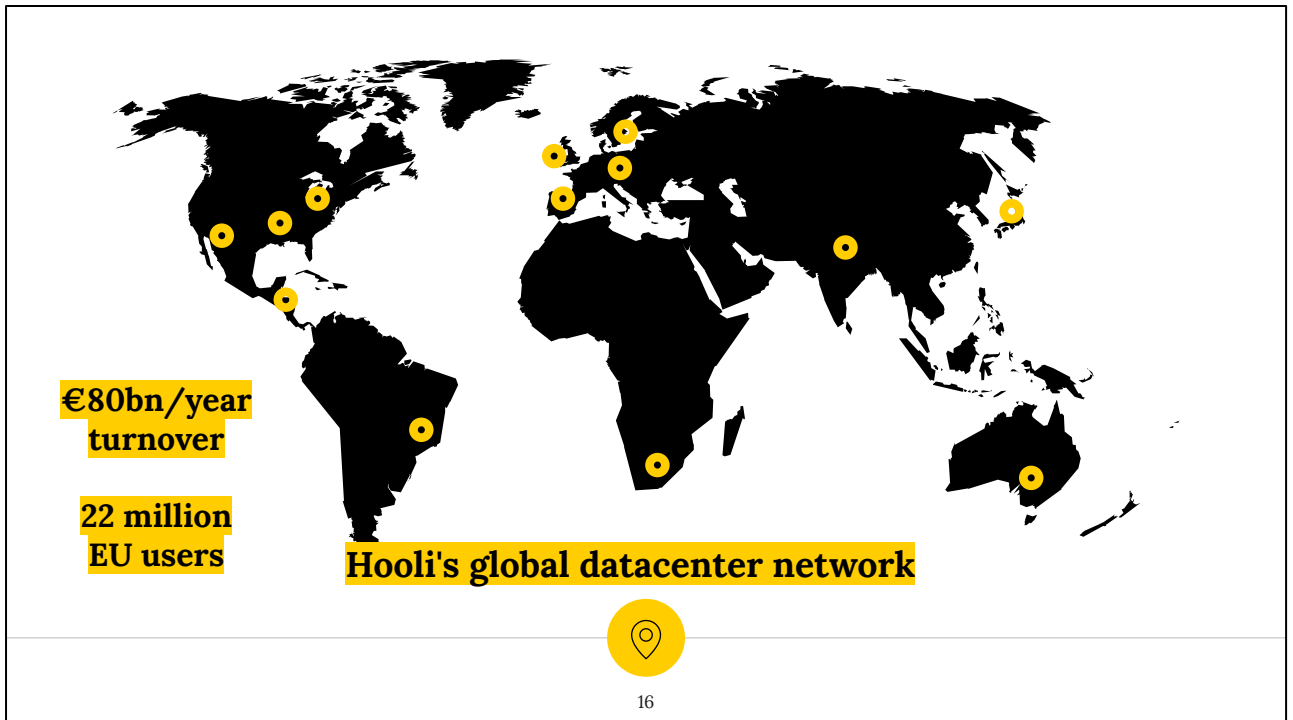


Hooli is about people

"Making the world, a better place, through minimal message oriented transport layers"

Let's consider what this means to everyone's favourite tech company, Hooli!

Hooli are a large company, with offices in 20 countries around the world. Many teams are spread over multiple countries, to give 24/7 support, and to make it easy for the world's best talent to work for them. Many work remotely from other countries.



They have giant datacenters in many countries, and have small caching "points of presence" in another 90 countries, to ensure their customers get low-latency access to their services.

They offer a wide array of products;

- Email & Chat
- Video
- Social Media
- Mapping services
- Targeted Advertising
-

Hooli have dozens of high-paid lawyers who have designed privacy policies and contracts that ensure they meet all of their GDPR obligations. They have decided to not hire employees in countries with rule-of-law problems, like Russia and China. They have a professional law-enforcement liaison organisation that makes sure only legal data requests are allowed.

How well do you think Hooli are doing, with respect to the GDPR ?



Who cares where data lives

If it can be accessed without independent oversight, data protection is not "Adequate".

17

If a Hooli engineer lives in a country where they can be required to share information on an EU citizen without independent oversight, perhaps under threat of an obstruction of justice charge, that is a breach. That is a problem with pretty much any product that requires personal information, metadata, etc.

If Hooli have employees in the UK, they are required to collect messaging metadata for the UK intelligence agencies.

The United States vs. Microsoft 2018 case has proven **problematic** for the EU to US transfers, and it remains to be seen how the UK will deal with a similar challenge. Any volunteers ? Anyone want to find out for us ?

Administrative fine: 4% of €80bn

Each breach.



Large companies have successfully held off or delayed administrative fines, thanks to systemic delays in DPAs and various courts. Most companies like Hooli don't see a 4% fine as being a real threat that could actually happen. To date, most fines have been far smaller.

20 million users

€1000 each

"A data breach is now an extinction level event"



19

While technically, companies have a huge exposure to compensation claims for losing people's data, we've not seen any in Europe.

If we did, very few internet-scale companies could survive. But with mass claims now being specifically legislated for, and a proliferation of grounds of claim with the new laws, the chickens (or other birds) are coming home to roost.

A little bit of foreshadowing there, for those who like that.



What could be done ?



22

You don't need to read all this. That's why we release the slides afterwards. But, to summarise....

To meet the spirit and letter of these new laws, Hooli should ensure that no EU resident's data is stored outside of the EU, or accessible to non-EU employees. They have a few options.

1. Create a company structure where the EU company is 100% independent of non-EU parent companies. No one in the EU reports to someone outside the EU.. so they don't have a manager that can be pressured by foreign governments.
2. Build & provision datacenters in Europe, or ensure that any data the EU company stores outside the EU is encrypted-at-rest with no keys leaving the EU.
3. Technology-licencing, where source code, IP, etc. is licenced from the EU company, to other companies, so EU entities cannot be forced to disclose data, or use compromised software in order to continue to function.
4. And lastly, any time US Hooli users interact with EU Hooli users, the software would have to work in a 'federated' way. Think of how Email allows you to send email anyone on the planet, because it uses a standardised API that doesn't require central control. Hooli will have to re-write it's Chat and Social Media systems with this in mind. This does not mean simply Mastodon-like

1. federation, because anyone who allows a user to create a post with personal information in it must be able to ensure that all copies of that post are deletable later.

Poll - who thinks their employer would go for "Re-home". What about Build ? And a licencing structure that sends all IP to Europe, then licences it back ? What about true federation?

Or respect human rights

Don't laugh. It's rude.

"Human rights could apply to everyone"



Another alternative is that more countries could see a social and economic benefit from bringing in privacy as a human right. It's surprisingly popular around the world.

4

This happened before.

Big tech impacted citizens safety in the early 20th century

22

For centuries, the human right to bodily integrity has been recognised, but not always enforceable, especially by those who worked in industries where profits were more important than employee safety, like mines and construction sites.

In the early 20thC century, as more and more citizens were impacted by large companies, countries brought in 'duty of care' laws, that allowed individuals to hold companies to account. <pause>

Injuries in workplaces and from consumer products, eventually had real impacts on the profitability and even survivability of companies.



None of these men could imagine a world where building sites were safe. They took that job, knowing that one in a hundred would die every year. Even as late as the 1970s, the average bridge construction in the United States claimed nine lives. The construction industry considered the minimal compensation for injuries and deaths as the cost for doing business.

No one in this audience could possibly imagine taking a job where it's normal to eat lunch in an unsafe environment like this.

None of those men could imagine a world where if any of them got hurt, or injured that the compensation would be so high that it would be cheaper for an employer to make the building site genuinely safe than, than risk a single serious injury.

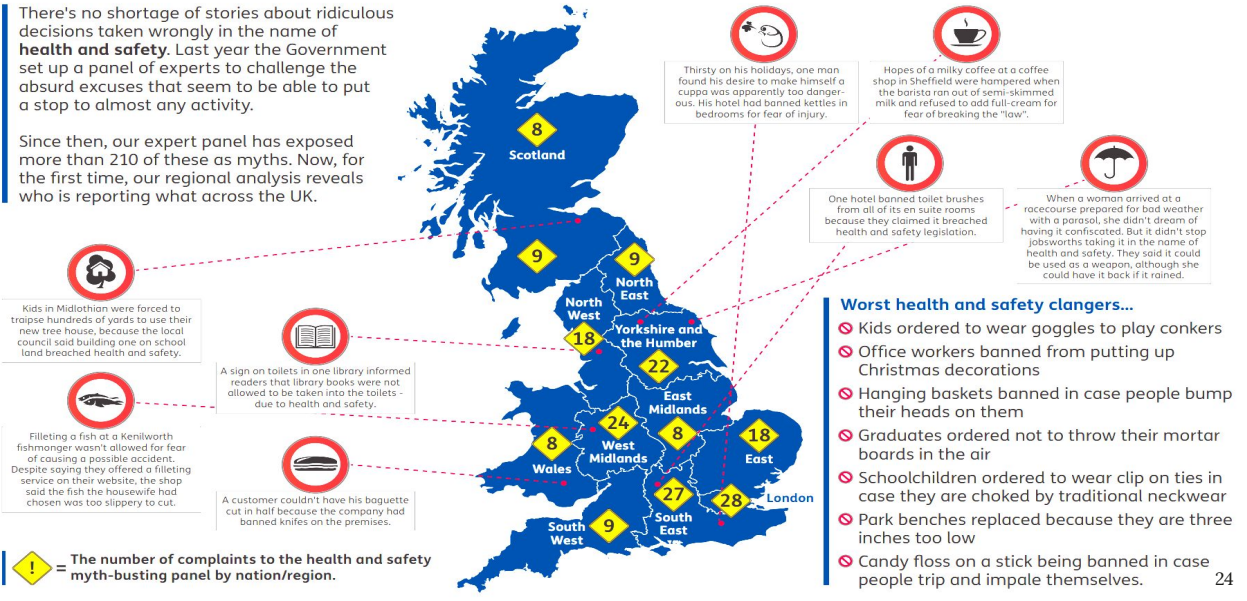
// Incremental change beats radical transformation

This transition took decades. To those paying fines, each incremental development felt outrageous and yet soon normalised.

Map of Elf and Safety Madness

There's no shortage of stories about ridiculous decisions taken wrongly in the name of **health and safety**. Last year the Government set up a panel of experts to challenge the absurd excuses that seem to be able to put a stop to almost any activity.

Since then, our expert panel has exposed more than 210 of these as myths. Now, for the first time, our regional analysis reveals who is reporting what across the UK.



- Worst health and safety clangers...**
- ⊗ Kids ordered to wear goggles to play conkers
 - ⊗ Office workers banned from putting up Christmas decorations
 - ⊗ Hanging baskets banned in case people bump their heads on them
 - ⊗ Graduates ordered not to throw their mortar boards in the air
 - ⊗ Schoolchildren ordered to wear clip on ties in case they are choked by traditional neckwear
 - ⊗ Park benches replaced because they are three inches too low
 - ⊗ Candy floss on a stick being banned in case people trip and impale themselves.

This slide is a genuinely strange co-publication of the UK Department of Work & Pensions and the Health & Safety Executive.

It shows that the backlash against "health and safety" never completely ended. This is a recent publication from the UK government, taking offence at often valid safety concerns of workers.

The backlash against data privacy will be the same.

We need to recognise that voices can continue to object to change, but over time will find themselves moving from the mainstream to the fringes.

Building sites will continue to require hard hats and messaging providers will continue to roll out encryption.

What if respecting people's privacy was a business advantage ?

Are you eating your lunch, sitting on a new girder ?



25

Today's data industry is similar to the construction industry of the 1930s; before workers could sue directly for physical injury at work.

An industry with little competence at protecting workers found it difficult and expensive to systematise those protections.

Over time, it became a competitive advantage and eventually utterly normalised.

Data Protection is the world's newest fundamental right, and the most significant addition to fundamental rights since world war two. This learning process will be as difficult, and resisted, because it impacts the data industry, governments, and even the products consumers are allowed to use.

You all know of companies that have threatened to withdraw services in Europe unless they are allowed to break the law.



Human Rights-based Privacy is ...

Ambiguity of Privacy 'Right'

Vaguely defined
Conflicts with other Human Rights

Expensive

Exchange of data underpins Internet economy
Regulatory burden ratchets up

Anti-innovation

Regulatory barriers to entry
Stifling technological progress

Politically driven

Empowers Bureaucratic power
Risks freedoms of expression and speech

Limits personal freedoms

Denies Individual Autonomy
Interferes with Market Mechanisms for Privacy

Privacy is a Luxury Good

Differing Cultural Norms around Privacy
Limits access to free services

Get ready for very expensive PR companies to be hired to produce better quality propaganda against privacy, than the Department of Work & Pensions paid Alan Partridge to come up for their poster we saw earlier.



- In 1965, Ralph Nader called out manufacturers of unsafe cars for accepting avoidable deaths in the name of profitability
- He was attacked by car companies; they denied the truth, and later had to explain their immoral calculus at senate subcommittee hearings
- Economists at the time argued that trading safety for affordability was acceptable because people needed cars to go to work
- There was 'Whataboutery' - why did he just attack Chevrolet ? Why not other dangerous cars ? Is it just because he owned stock in Chevy's competitors?
- Nader's book was called out, as recently as 2005 by a Conservative newspaper, as one of the "most harmful books in the 19th&20th centuries", along with Mein Kampf, Silent Spring, and The Origin of the Species

In case you were wondering what I meant, when I suggested anti-change arguments would be sustained by the fringe for decades.

Expect people to attack the fundamental right to privacy in a similar way.

- Companies will insist they are respecting privacy, while the problems we mentioned will still be ubiquitous
- Experts of all sorts will attack these laws as being unworkable, unenforceable, uneconomical, etc.
- People already ask why is the EU singling out successful US companies - is it political ? Do they hate success ? Are they trying to destroy the internet ? No. The courts want to take a small number of specific examples, to drive culture change

But there is one last change driver, and it never fails to work over time. Can you guess what it is ?

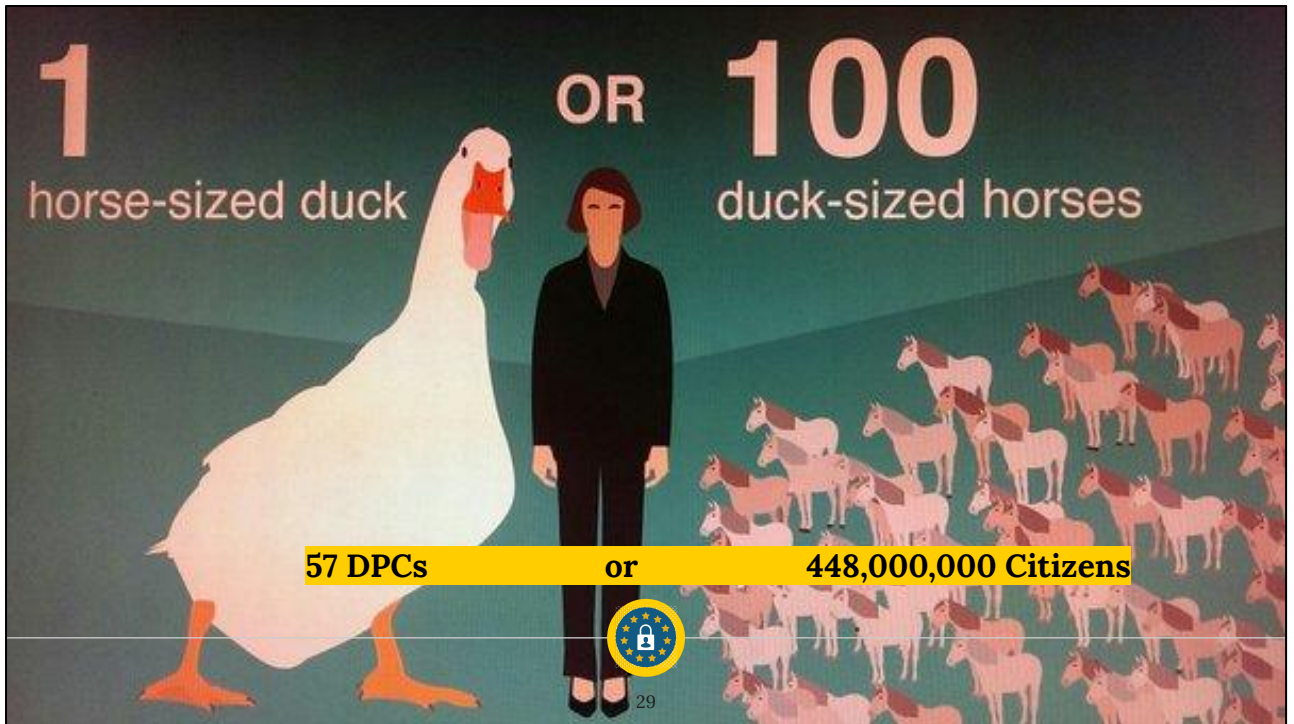
*Can the Data Protection
Commissioners take on all the
companies at once ?*



We mentioned earlier that there was a big delay between the idea of, and the ubiquitous implementation of, the right to bodily integrity. Look up the 1932 case about "the snail in the bottle" - the first time this concept was dealt with in the English language courts. That's your homework.

The key driver of change was allowing citizens legal standing in court. Instead of government regulators suing companies for privacy breaches, the EU's new law on Collective Redress is going to change the nature of the battle for privacy.

<giant pause>



Collective redress means that companies will no longer have DPCs as a primary threat, waving fines of a few percent of global turnover every so often.

Instead, they will be attacked by millions of citizens, each looking for a few hundred, or a few thousand euro each.

This will be far too expensive to litigate; an enormous evolutionary pressure will force all companies to deal with it by slow, coordinated, and fundamental changes in their business models.

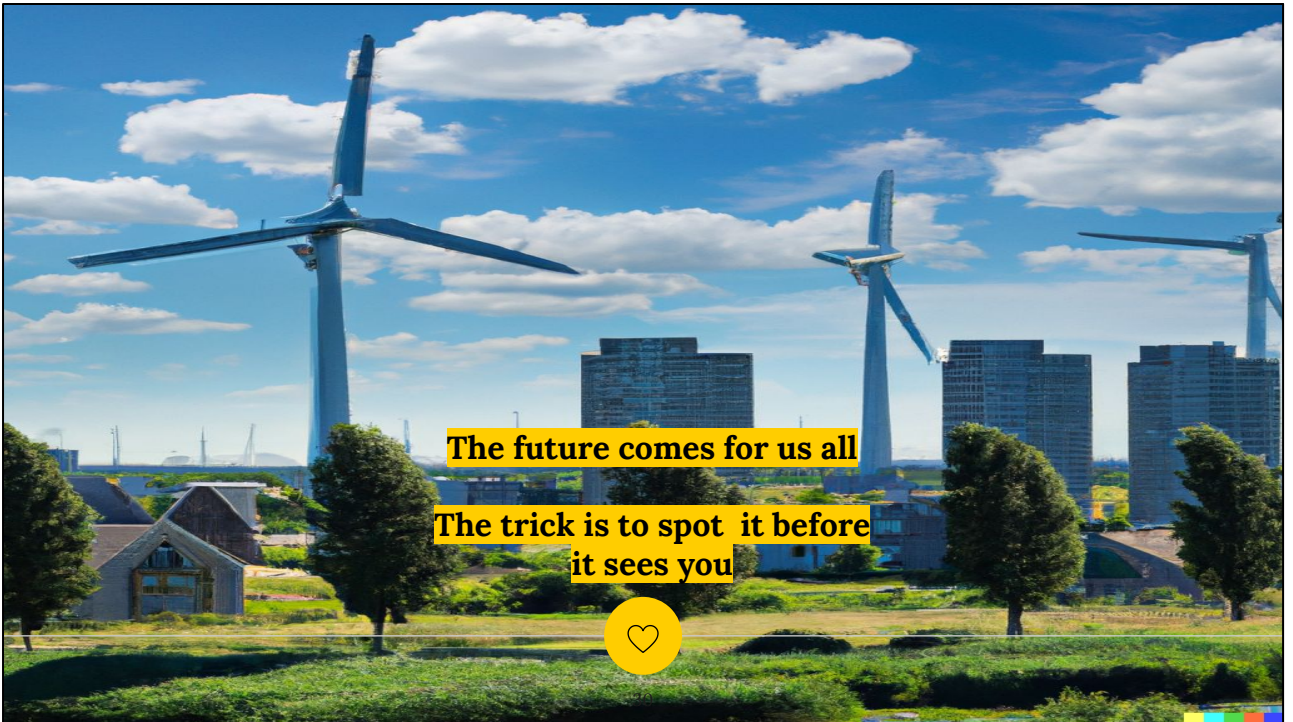
This is the same evolutionary pressure that gave us building sites with hard hats, steel toecaps....and portacabins to eat lunch in.

It's what gave us cars with seatbelts and unleaded petrol.

It gave us restaurants with separate chopping boards for raw meat & salads.

It gave us doctors who count their scalpels after a surgery.

It's a powerful force to be embraced.



The future comes for us all

**The trick is to spot it before
it sees you**



I've talked a lot about the past; the wrongs of the past, and the lessons we've taken from them.

I've mentioned some interesting changes that are happening right now.

Humans great ability is the power to recognise patterns, and use them to predict the future. To keep themselves safe.

There is no reason our industry can't do the same. We are very smart. When we want to be.

And this is where I'd intended to leave my talk. Except, sometimes the future comes at you faster than you expect.

Brussels, 10 October 2023

Dear Mr Musk,

Following the terrorist attacks carried out by Hamas against Israel, we have indications that your platform is being used to disseminate illegal content and disinformation in the EU.

Let me remind you that the Digital Services Act sets very precise obligations regarding content moderation.

First, you need to be very transparent and clear on what content is permitted under your terms and consistently and diligently enforce your own policies. This is particularly relevant when it comes to violent and terrorist content that appears to circulate on your platform. Your latest changes in public internet policies that occurred over night left many European users uncertain.

Second, when you receive notices of illegal content in the EU, you must be timely, diligent and objective in taking action and removing the relevant content when warranted. We have, from qualified sources, reports about potentially illegal content circulating on your service despite flags from relevant authorities.

Third, you need have in place proportionate and effective mitigation measures to tackle the risks to public security and civic discourse stemming from disinformation. Public media and civil society organisations widely report instances of fake and manipulated images and facts circulating on your platform in the EU, such as repurposed old images of unrelated armed conflicts or military footage that actually originated from video games. This appears to be manifestly false or misleading information.

I therefore invite you to urgently ensure that your systems are effective, and report on the crisis measures taken to my team.

Given the urgency, I also expect you to be in contact with the relevant law enforcement authorities and Europol, and ensure that you respond promptly to their requests.


Moreover, on a number of other issues of DSA compliance that deserve immediate attention, my team will follow up shortly with a specific request.

I urge you to ensure a prompt, accurate and complete response to this request within the next 24 hours. We will include your answer in our assessment file on your compliance with the DSA. I remind you that following the opening of a potential investigation and a finding of non-compliance, penalties can be imposed.

Yours sincerely,

Thierry Breton



Following the terrorist attacks by Hamas against , we have indications of X/Twitter being used to disseminate illegal content & disinformation in the EU.

Urgent letter to @elonmusk on #DSA obligations 

What could be the worst way to respond to an EU regulator ?

This is the first time I've seen the Commissioner for the Internal Market talk about enforcing the Digital Services Act. It's very exciting. Unlike the GDPR, this isn't being enforced via national DPCs.



Elon Musk   @elonmusk · 12h ...

Our policy is that everything is open source and transparent, an approach that I know the EU supports.

Please list the violations you allude to on X, so that that the public can see them.

Merci beaucoup.

 2,105

 5,222

 22.4K

 1.4M



Tell me you are a billionaire who is used to politicians agreeing with them.



Thierry Breton  @ThierryBreton · 10h

Vu, merci.

You are well aware of your users' — and authorities'— reports on fake content and glorification of violence.

Up to you to demonstrate that you walk the talk.

My team remains at your disposal to ensure DSA compliance, which the EU will continue to enforce rigorously.

 1,786

 786

 3,352

 366.4K



That demonstration is due 19:00 tonight.





Thanks!

Any questions ?

You can find me at

- john.looney@gmail.com
- [@bigvalen@mastodon.ie](https://mastodon.ie/@bigvalen)

Right. Any questions ?