LinkedIn

Misleading Advertising - A PET Pain! Why it's time to re-name Privacy Preserving Technology/ Techniques and Call Them What They Are...

Judith Ratcliffe, CIPP/E

February 7, 2023

What are the things that are currently called Privacy Preserving Technology/ Techniques (also often called Privacy-Enhancing Technology/PETS)?

The list from The Royal Society includes:

1) Trusted Execution Environments

2) Homomorphic Encryption

3) Secure multi-party computation (PSI/PIR)

4) Federated Learning/ Federated Machine Learning

5) Differential privacy

6) Privacy-preserving synthetic data

You will note that even 5 and 6 in this list appear to have been erroneously labelled with the term 'Privacy' - this is arguably an incorrect label and should be disregarded by those who genuinely want/intend to protect the Privacy of the individuals whose personal data they want to collect and use.

Why don't they actually 'preserve Privacy'?

Note: so we are all 'on the same page' wherein I say 'means', next to each of the techniques below, I have presented the definition, as appears to be given in The Royal Society's report:

https://royalsociety.org/-/media/policy/projects/privacy-enhancing-technologies/From-Privacy-to-Partnership.pdf

1) Trusted Execution Environments means 'securely **outsourcing** to a server, or **cloud**, computations on **sensitive** data'.

Alarm bells will ring for any Privacy Professional in relation to the parts of the definition I highlight in bold.

Calling something 'trusted' does NOT make it trust-worthy or reliable.

Your Organisation may 'trust' an outsourced provider, but are they truly trustworthy?

The very action of sharing personal data with Outsourced Providers and Cloud Providers may break the Confidentiality of the personal data and subsequent deliberate and /or accidental actions and ommissions by those Providers may cause further personal data breaches and invasions of Privacy, which harm individuals, such breaches may include but are not limited to Governments in Third Countries unlawfully accessing the personal data, unexpected teams (including analytics teams and machine-learning teams) viewing and accessing personal data and using it in unexpected ways. (The 'computations' themselves may be a cause for concern.)

Outsourced Providers can increase risks of harm to individuals and there can be a lack of appropriate control over the actions of those providers by Data Controllers, which increases risks of Confidentiality and Data Integrity Breaches.

A number of Cloud Providers appear to seek to use copies of personal data for 'their own business purposes', which can be unexpected and unwelcome to the individuals to whom the personal data belongs.

The Cloud is known to leak - How many breaches have hit the headlines in recent years, alone? How many more haven't been notified even to Supervisory Authorities?

Sensitive personal data, in particular, attracts extra protections under the Law and arguably shouldn't be being proposed for use, nearly so lightly.

The more sensitive the data, the more harmful negative impacts may be on those to whom the personal data belongs.

One Core Privacy Question that The Royal Society appears to have failed to ask is - Should we actually be providing (and/or seeking) access to that data in the first place?

2) Homomorphic Encryption means 'securely outsourcing specific operations on sensitive data; Safely providing access to sensitive data'.

Again we have the issue of access that has **not** (in all likelihood) been authorised by the individual to whom the personal data belongs, plus confidentiality breaches and then data integrity breaches and further confidentiality breaches when the 'operations' are performed on the data.

One Core Privacy Question that The Royal Society appears to have failed to ask is - Should we actually be providing (and/or seeking) access to that data in the first place?

Add to that the fact that 'encryption' is no guarantee of prevention of access. As in the Encrochat Case, where Europol decrypted a supposedly undecryptable network, encryption appears to be easily breakable by those who are motivated enough to attempt it.

https://www.europol.europa.eu/media-press/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe

3) Secure multi-party computation (PSI (Private Set Intersection) PIR (Private Information Retrieval) means 'enabling joint analysis on

sensitive data held by organisations'.

Even Microsoft Azure, openly states that 'the data being shared [by some Secure multi-party computation systems] is confidential. The data may be personal information, financial records, medical records, private citizen data'

https://learn.microsoft.com/en-us/azure/confidential-computing/use-cases-scenarios#secure-multi-party-computation

Again the clue about the fact that such technologies and activities *break Privacy* instead of enhancing it, is in the fact that they appear to use 'sensitive data', with no mention of obtaining fully informed consent from individuals beforehand.

Unlawful repurposing/extra unexpected use appears to be happening, here.

Another clue is in the fact that they are proposing to allow that sensitive data to be analysed by many 'parties', which means that again the Confidentiality and Integrity of that data appears to be automatically put at risk.

Azure states that 'For example, using machine learning for healthcare services has grown massively as we've obtained access to larger datasets and imagery of patients captured by medical devices'.

https://learn.microsoft.com/en-us/azure/confidential-computing/use-cases-scenarios#secure-multi-party-computation

This also gives rise to questions about breaking the Common Law Duty of Confidentiality in relation to Patient data, too.

Azure goes on to say that *'Multiple sources can upload their data to one enclave in a virtual machine. One party tells the enclave to perform computation or processing on the data. No parties (not even the one executing the analysis) can see another party's data that was uploaded into the enclave.*

In secure multi-party computing, encrypted data goes into the enclave. The enclave decrypts the data using a key, performs analysis, gets a result, and sends back an encrypted result that a party can decrypt with the designated key.'

First of all the Confidentiality of the Data (and possibly also Data Integrity) appears to have been breached by the teams that have harvested the personal data in order to put it into the enclave and also the enclave is still a third party that appears to see/access all of the parties data and all of the data is decrypted within it and because of that, further Confidentiality issues arise.

The results may also contain personal data, albeit perhaps in an aggregated form and therefore the personal data is still likely to be subject to Data Protection Laws.

There is also high potential for unfair stereotyping and discrimination within the produced 'analysis' or 'model'- What big AI projects and analysis projects tend to forget is that, particularly with health, individuals are individuals, with differing health and treatment needs that arguably no predictive machine/ profiling will pick up on - For example, I strongly suspect that they wouldn't pick up on an individual's allergies to particular medicinal products. They

may also miss specific family-related issues and environmental issues (e.g. problems with particular unintended substances in water supplies, where they hadn't been pre-programmed into the AI...)

A machine will only compute from the data you put into it, and all the data in the world will not tell you the things that a person will only voice to another person.

For these reasons, the supposed benefits, may not actually be so beneficial as all the hype wants us to believe and I consider that a healthy dose of scepticism needs to be administered.

4) Federated Learning/ Federated Machine Learning 'enables the use of remote data for training algorithms, data is not centralised'.

Again, just because 'data is not centralised', doesn't mean you haven't broken people's Privacy. You break Privacy everytime you collect/ use someone's personal data for things they don't want you to use it for/ aren't expecting you to use it for. You break their Control over how Private things are. You break the Confidentiality of their personal data and that matters, especially if those private things are hurting them, in some way. People feel violated when they learn that their private things or parts of them have been sucked into another system for further uses.

Risks of personal data being stolen by hackers, or breadcrumbs leading back to identifying individuals appear to remain present.

Clearly also, since 'personalisation' can sometimes be intended through e.g. 'meta learning' if what I've read is correct, then profiling and targeting and stereotyping are also happening- These also break a person's Privacy Rights.

And that is without going into the 'ins and outs' of Article 22 GDPR- The Right NOT to be subjected to automated decision-making, including profiling, which has legal/ other similarly significant effects...

5) **Differential privacy** is said to 'prevent disclosure about individuals when releasing statistics or derived information'.

For starters, you will note that on P19 of The Royal Society's report, it confirms that it is a 'security' definition - In that case, I would argue, the name 'Privacy' shouldn't feature at all.

The part of the name 'privacy' in 'differential privacy' appears misleading and may also cause data scientists and others to think that they can give different individuals and/or different bits of personal data, different levels of Privacy, which is highly likely, in my view, to cause them to indulge in overly risky behaviour and they may cause serious harm as a result.

It doesn't prevent personal data being used for statistics, when someone has objected/ 'said no' to use for that whether at the time of collection of personal data/ or afterwards. It doesn't keep personal data within the statistics system, before and while they are generated, to a minimum. It doesn't stop Confidentiality or Data Integrity Breaches while the personal data are being used to generate the statistics (or even before that) and it doesn't appear to stop hackers hacking in, either.

The inferences generated may be misused to stereotype/label people and may also get things wrong and, as many Privacy Professionals have warned,

previously, pseudonymised data, which appears to be what may be spat out at the other end, can still be used to re-identify people by reasonably motivated people and even by well-intentioned people who are familiar with local areas and/ or who simply join the dots/ can fill in the blanks. So-called Differential Privacy actually may not keep things as private as appears to be claimed...

6) **Privacy-preserving synthetic data** is said to 'prevent disclosure about individuals when releasing statistics or derived information'.

At least The Royal Society's table on P17 confirms 'Privacy enhancement unclear' for (6).

It's the 'generated from real-world data' definition on P19 of The Royal Society's report that gives me pause. As with all the other so-called PETS, the actual Privacy 'enhancement' and 'preservation' may be considered questionable and Confidentiality and Data Integrity breaches appear highly likely to occur. Where original data is changed and or accessed/viewed when it shouldn't be, Privacy is Violated, Personal Data Breaches happen and harm can be caused.

The truth seems to be that none of those so-called PETS (at 1 -6, above) preserve Privacy or enhance it, at all.

They break it.

Because What is Privacy?

- It is the Right to prevent your deeply personal details being used for things you don' t expect.
- It is The Right to be able to access Health Services WITHOUT treatment being held to ransom for your personal data and/or only being treated/ helped if you hand over excessive amounts of personal data and /or if you permit use of your personal data for unwanted and /or unexpected purposes.
- Privacy is the Right NOT to be profiled/ stereotyped /discriminated against or have 'personalisation' and 'personalised products' thrust upon you - the Right NOT to be told 'what you like/ should do' with your life by others.
- Privacy is the Right to keep deeply personal and private things OFFline to prevent misuse and abuse and unintentional or intentional sharing (even internally) and cyber risks like hacking.
- Privacy is the Right to go about our business unmolested by the State and Commercial Organisations.
- Privacy is the Right to be Left Alone and NOT to have Our Reputations unfairly tarnished or stigmas attached to us because a biometric system 'doesn't like the look of us'.

These are just a few examples of your Privacy Rights and they appear NOT to be either preserved or enhanced by The Royal Society's so-called PETS, rather, they appear to be undermined and broken by them (as I hope I have demonstrated). The PETS appear NOT to be Privacy-Enhancing or Privacy-Preserving, at all, they appear to take away your Privacy and remove your Right to Say No and Your Right to Control over your personal data. As well as denying you the most basic of Privacy Rights, they also appear to encourage oversharing, misuse of your personal data and denial of Your Rights over your personal data.

Why must Organisations Stop misleading Individuals and other Organisations about so-called PETS?

Because as well as breaking Privacy and Data Protection Laws, and also, arguably Consumer Protection and Competition Law, by failing in your duties of fairness towards Consumers, you may also be breaking the Trade Descriptions The Business Protection from Misleading Marketing Regulations 2008 and fall foul of the clear guidance/ rules set out by the Advertising Standards Authority, too around Misleading Advertising (both to Organisations and to Consumers/ Individuals).

2008 No. 1276 TRADE DESCRIPTIONS The Business Protection from Misleading Marketing Regulations 2008

Part1, definitions and prohibitions

Prohibition of advertising which misleads traders 3.

—(1) Advertising which is misleading is prohibited.

(2) Advertising is misleading which

— (a) in any way, including its presentation, deceives or is likely to deceive the traders to whom it is addressed or whom it reaches; and by reason of its deceptive nature, is likely to affect their economic behaviour; or

(3) In determining whether advertising is misleading, account shall be taken of all its features, and in particular of any information it contains concerning

— (a) the characteristics of the product (as defined in paragraph (4));

— (d) the nature, attributes and rights of the advertiser (as defined in paragraph (5)).

(4) In paragraph (3)(a) the "characteristics of the product" include

(b) nature of the product; (d) composition of the product;

(g) fitness for purpose of the product;

(h) uses of the product;

(j) specification of the product;

(l) results to be expected from use of the product.

(5) In paragraph (3)(d) the "nature, attributes and rights" of the advertiser include the advertiser's— (a) identity; (b) assets; (d) ownership of industrial, commercial or intellectual property rights.

P4 MISLEADING AND AGGRESSIVE COMMERCIAL PRACTICES: NEW PRIVATE RIGHTS FOR CONSUMERS Guidance on the Consumer Protection (Amendment) Regulations 2014

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/721872/misleading-aggressive-commercial-practices-guidance.pdf

Misleading actions

The 2008 Regulations make misleading actions unlawful (see regulation 5). An action by a trader is misleading **if it contains false information or if it is likely to mislead the average consumer *in its overall presentation*.**

For example, the information could be about the main characteristics of the product (like its benefits or composition), and the consumer's rights or the risks he or she might face.

Regulation 5(4) of the 2008 Regulations includes a list of the matters covered. Examples Misleading broadband speed advertisements:

A consumer takes out an expensive 18 month broadband package advertised with speeds of "up to 24 MB". *In fact, it was never possible for any customer to achieve this and average speeds were less than half.*

In the same way, products that claim to enhance and/or preserve Privacy that don't genuinely do this, may also be considered to break the 2008 Regulations.

What does the Advertising Standards Authority say?

ASA Rule 3.1: https://www.asa.org.uk/static/uploaded/eac4324b-779b-487c-9e1d7d0f7acd488a.pdf

*3.1 Advertisements **must not materially mislead** or be likely to do so.*

*3.2 Advertisements must not mislead consumers by **omitting material information.** They must not mislead by hiding material information or presenting it in an unclear, unintelligible, ambiguous or untimely manner.*

***Material information is information that consumers need** in context **to make informed decisions** about whether or how to buy a product or service.*

What should real PETS look like?

I will examine what Genuinely Privacy-Preserving Technologies and Techniques and Genuinely Privacy-Enhancing Technologies and Techniques look like in another articles, but suffice it to say, here, that they are things that give YOU the power to choose and control what happens to you/ your data (including images of you)/ your body/ your life and protect your reputation.

What can we conclude?

I would argue that all Organisations, particularly those with significant amounts of power and weight in Civil Society have an even greater duty NOT to mislead the Public and have an even greater duty to encourage the protection of our Privacy and Our Rights and lead the way in doing so.

For the moment, until PETS are truly what their name claims them to be, always 'dig a little bit deeper' and check against what Privacy actually is, before you make what could be a very costly mistake in terms of:

1. **Your Wasted Costs (Paying for something that doesn't 'do what it says on the tin');**

2. **People Walking Away from you, because you made a promise that you were Preserving/ Enhancing their Privacy, but your technology let you down and you broke your word;**
3. **Loss of Customers, Bad Reputation, Loss of Employees and Potential New Customers Avoiding You/ Fleeing to Your Competitors...**

I would encourage all Organisations, rather then making what will arguably be false and/ or misleading claims about protecting Privacy, which will cause a loss of Public Trust, Reputational Damage and ultimately even possible legal sanctions in the longer term (and perhaps the shorter term, too), to genuinely preserve and enhance Privacy (including but not limited to Data Protection) by:

1. Keeping the collection of personal data to what is strictly necessary and proportionate and minimal - Set up your systems, processes and policies to make this happen, every time.
2. Avoiding further uses/ unexpected uses of personal data unless and until you have obtained the fully informed and explicit consent of individuals first - Set up your systems, processes and policies to make this happen, every time.
3. Making sure your systems can destroy data and correct data on command, every time.

And those are just 3 simple things to start your Privacy preserving/ enhancing journey, which will also remove the need to buy ever increasing volumes of costly technology that may also use more electricity and increase environmental harms.

Isn't It Time to Raise The Standard and Make Privacy-Preserving and Privacy-Enhancing Technology and Techniques do what they say they will and do what Members of the Public, arguably, expect.

#TimeToChange #PrivacyPreservingTechniques #PrivacyPreservingTechnology #MisleadingAdvertising #AdvertisingStandards #PrivacyMatters