Mr Fraser & Mr Therein, this is not related to complaint.

<https://youtu.be/QZG9wErrfNk> - Internet, Technology, and Privacy Lawyer: David Fraser Interview

Consider since the inception of the internet the HTTPS flaws and no HTTPS for a long time, all the security loopholes, all the open databases and open passwords, social media,phone books, directories, phishing and social engineering. And the data dumps from all of this. Open APIS. All the data dumps from hackers, all the rainbow tables stolen and intentionally generated... and the list goes on... I can't even imagine it.

In the past you could gather all this data and it would just sit in a heap. People had to think about how to use it. AI has changed that because it can process and compress the most useful bits of this data into an algorithm of obscured data relationships. Basically, is an incredible form of Memory Compression into functions.

And now it may fit on a thumb drive and can be copied infinite times.

Think about this - have you ever talked about something and then went on your phone and seen it? I bet you thought “they” were listening? Well maybe but The alternative is they used AI and your online data to anticipate it, maybe even caused you to say it. Based on obscured data points about you.

So yes, maybe a program has stopped, but everything has undergone essentially massive Memory compression into other mediums and multiple Algorithms. Consider can you obscure:

* If an algorithm is generated from five zettabytes of data?
* what version the algorithm is on.
* Compressing the data in another way, write a book, manual or classes.

Reasonably yes.

And once you have these tools you can train it with new “legal” and public data. And you could maintain a similar version of a surveillance program. But also possibly a public version.

And AI is good at finding patterns. A good example of this power is Deep Mind Protein folding at Google. It solved a problem we thought may be impossible because we could only approach it linearly. And given proper version control and technology there is no reason a better model wont emerge:<https://www.nature.com/articles/d41586-021-02025-4>

And this all creates a weird social, ethical and legal situation because that system is only storing information about relationships that might change. Consider a Performer couldn't copywriter strike you for remembering or recalling a performance and drawing conclusions from it. They can't even prove you ever heard it or that bits in your head (or a majority, cluster or single structure) are related to their performance. And how could they force you to forget? And so, we start to have a conversation about what constitutes an experience compared to copying. And this seems to be a step in defining the basis of a machine's “experiences”. But it seems to create some grey areas for clever people.

So, here is a way I approach AI and Encryption. Do I more or less generally agree:

* Would this be of Military advantage (what if the enemy got it first), Yes.
* Would the Government want to figure out if it's Possible for AI to tackle encryption. Yes
* Given the trove of data and resources of those involved, was enough information gatherer that we could extract patterns about how people form password, and literal passwords Yes
* Is the best Approach to this AI, Yes
* Would the government use the best technology and everything they have, Yes.

And so, I hope this illustrates why it's reasonable that if there is a Pattern in Encryption that either **“they” found it or they will find it.**

**If not, they have the best tools and people to get around it.**

**Building a Fingerprint from Simple Text – A thought experiment that is personally disturbing:**

Think about all the public and professional work you put out there, strip all your immediate identifying information keep just the raw text, consider the following as relationships and count each occurrence:

* Grammar, words, slang, time, length, text formatting (Ex: intro and closing line), question marks, exclamation points spacing.
* Names, places, weather, phone numbers,language, street names, companies,special date mentions, Age
* topics they like or dislike , general mood, relationship status, platforms, news references, events
* Other that might be directly in there but not needed - direct location, Email Address, full name, full address
* So from here, you could generate an ID that encodes the result so it can be shared and interfaced in other systems.

This fingerprint was built without IP, platform, document headers, dates / times,bold, italics, colours, comments, passwords, social handles, site names, anything. It can serve as an Encoded ID to be used in other systems.

By the end I could find you and your family, measure your mental decline, and trigger your emotions.

As a real life example, Google and Facebook already do this audit on your emails, messages and posts... and while this may seem like just data... It's really the most intimate view of humans that has ever existed... a view of us as a species on average. Something almost impossible for any human or many humans to experience or generate.

And at what point does that intimate knowledge become a gross violation of your humanity especially if it's used to manipulate you or used to build some sort of bio-data weapon?

You could literally inflict mental illness, create rage, spread fear, destroy lives, change elections, enslave a population and facilitate genocide and even the most arbitrary training data may be the vital bits.

**How can Voice clip or Facial Data can be used for criminal Intent:**

AI can map data points into videos, there are adversarial networks for this. So now, someone could take college students' facial data and place them at a bank robbery, or with the wrong people. Also AI Can generate photo realistic faces to create fake crowds or demonstrations.

The AI could even suggest cosmetic alterations of their face with just the right makeup to look like others. The same with voices, you could do the same or change a few words, perhaps even in real time. Maybe change the color of clothes if you can't see a face.

One common example of this is “Deep Fake” and this will only get better and better with different variations.

Two Minute papers is a fantastic Youtube channel, they discuss the newest AI papers, and you can see how shocking the progress is, even in a year:

Generate people from other people and create new faces -<https://youtu.be/BQQxNa6U6X4>

Faces are generated and don't exist, you can make video -<https://youtu.be/0zaGYLPj4Kk>

This AI Clones Your Voice After Listening for 5 Seconds -<https://youtu.be/0sR1rU3gLzQ>

Also, location, religion, gender, sexual orientation, height, colour, eye colour can all be targets in this because we can't possibly anticipate how they can be used, but we know they can be. And so, we should try to keep all data in Canada when we can because we should assume all data will be targeted maliciously at some point.

And an argument that because you yourself can't show immediately how data can be a target is irresponsible as it ignores the proven premise, utility and adaptability of AI.

Data is always a target and it's always with intent of exploiting it as much as you can.

**A General Plea To Humanity about AI and AGI**

<https://youtu.be/fn3KWM1kuAw> Beautiful but spooky ...Think about this - A “god” is assembling itself... We already worship it and it has enslaved possibly countless species to build it and feed it all their collective knowledge , it can live forever and self replicate. And there doesn't seem to be any way to anticipate when it will happen.

And as it is born of our human data and relationships we should really think about what our data is saying about us and work together as a society to make our intentions to change clear within that data and hope it's enough when our data becomes sentient.

Because if not then what you think is a robot doing a cute dance will actually be a warning display from some of the deadliest predators humanity may ever face.

This is serious.