**The Definition of Differential Privacy - Cynthia Dwork**

Privacy preserving data analysis.

* Question: how to analyse data while preserving privacy? At least a 50 year old question.
* Many people think of de-identifying the data.
  + Original database 🡪 “de-identified data” set
  + But “de-identified data isn’t”. What does this mean? Either it isn’t data, or it isn’t de-identified.
* Next idea: “just Statistics”.
  + You want to just do data analysis, so why don’t you just release the statistics? Say the data analyst were to ask for, say, the number of people over 6 feet tall who like donuts (or something like that), and receives an answer, and then sends another query, gets an answer, and so on.
  + Fundamental law of information reconstruction: “overly accurate” estimates of “too many” statistics is blatantly non-private.
* What kind of privacy/guarantee are we trying to make? Can’t learn anything new about patients? The data analyst, after looking at the data set, mustn’t be able to learn anything new about the subjects that they didn’t know before having access to the data set.
  + But if we can’t learn anything new then what is the point of the data set?
  + We’re doing the statistical analysis of data to learn something new about the population.
  + But is learning something new a privacy compromise? No, we would have learned the same things had subject A have been replaced by another random member of the population; we’re not learning about subject A, we’re learning about people.
  + With this approach, we can disentangle learning about the population as a whole from learning about the individuals in the data set. This doesn’t mean that learning about the population as a whole can never hurt an individual.
    - E.g.
  + We’re not saying that we haven’t learned something that can be used against them.
* The English definition of differential privacy says that “the outcome of any analysis is essentially equally likely, independent of whether any individual joins, or refrains from joining, the dataset. We’ll learn the same things with the same probabilities.
  + DP separates thew harms that can come from the teachings of the database from the harms that can come from participation.
  + Suppose that a data set teaches us that smoking causes cancer, and that it’s known that person A smokes. This person’s insurance premiums may rise; they’ve been harmed by the teachings of the data set.
    - But they would be harmed in this way (the premiums rising) regardless of whether person A is in the data set of out of the data set.
    - And learning that smoking causes cancer is the ENTIRE POINT of statistical data analysis.
    - With this in mind, in this scenario, person A can be helped by the data set because they may be inspired to quit smoking.
* Formal definition of differential privacy:
  + First we need the concept of adjacent data sets.
    - Data sets that are almost identical; one is slightly smaller than the other and the larger one contains the data of just one more person.
  + *M* gives ε-differential privacy if for all pairs of data sets *x, y* differing in the data of one person, and all events *S*

Pr[M(x) [within set symbol] S ] =< e^ ε Pr[M(y) [within set symbol] S ]

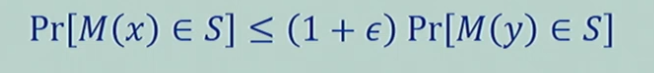
Where:

* M introduces the randomness.
* Algorithms that will analyse data sets will flip coins. They will be randomise algorithms.
* The algorithm/mechanism *M* gives epsilon-differential privacy if for all pairs of data sets *x, y* that differ in the data of just one person (i.e. x and y are adjacent data sets) and every possible output event *S*, the probability that we see S when the data set is x is almost the same as, it is at most RHS of the equation: it is at most e^epsilon \* the probability that we see S when the data set is *y.* so the ratio of these two probabilities is at most e^epsilon. And the probability space is over the coin flips of the algorithm.

The algorithm is the good guy.

And because we said for all pairs of the data sets, the same inequality would hold if we were to swap x and y.

* + This definition was put forwards by Dwork, McSherry, Nissim and Smith in 2006.
* So e^epsilon when epsilon is small is about (1 + epsilon):



* So when epsilon is 0, it says that these 2 probabilities must be the same; when there is 0 probability loss, we also get 0 information about the data set.
* So, a subject may say “if a bad event is very unlikely when I’m not in dataset (y), then it is still very unlikely when I am in the data set(x).
* So epsilon is our measure of “privacy loss”.

Properties of differentially private algorithms:

* Future-proof:
  + Privacy comes from the process by which the outputs are generated, and if a data release is differentially private, that ratio of probabilities doesn’t change if someone who sees the output learns other auxiliary information or sees other data sets that will exist in the future.
* Automatically yields group privacy:
  + K\*epsilon for groups of size k; .
  + If an algorithm yield epsilon-differential privacy for a single individual, then it automatically yields k\*epsilon differential privacy for groups of size k. so if epsilon-dp is satisfactory for one person, it will be scalable for k people as well.
* (most importantly, Dwork says) Understandable behaviour under composition:
  + Understand the behaviour of privacy loss of DP under composition.
    - Can bound cumulative privacy loss over multiple analyses.
  + “the epsilons add up”.
  + “one crude bound shows us that in the WCS the epsilons add up; we can do better than that and that will be the subject of Guy Rothwells talk.”
* Programmable:
  + Because of the composition property which says that we can understand when we ask about many different statistics, we get that differentially private algorithms are actually programmable. That is to say in ordinary programming, you don’t just compute everything from ands and ors. What we do is build sub-routines and algs for smaller problems and the whole field of alg design is the creative and intelligent combination of different computational building blocks to carry out a sophisticated computational task while minimising some sort of resource usage (time or space).
  + The same thing is true w DP. You can take small differentially private building blocks and combine them to carry out complex Differentially P data analyses. And that is a power that no other approach has [as far as Dwork knows].
* Differential privacy has to somehow blur the answers a little bit. So we have truth and the blurred version of truth.