CIS399: The Science of Data Ethics	Lecture 17: Mar 21, 2019
Instructor: Michael Kearns & Ani Nenkova Gokhale	Scribes: Kevin Sim and Rounak

1 Approach To Privacy

We will be using an intellectual approach to privacy, similar to the one we used for fairness. That is, we will be examining different definitions of privacy and methods of ensuring privacy and evaluate them.

2 Typical Notions of Privacy

Most people would consider anonymity, private communication, confidentiality (user data is not shared to other parties), and ownership of data important aspects that privacy should cover. These are all important features that center around privacy. However, we are going to make a distinction between data security and privacy.

3 Data Security Vs. Privacy

Suppose we have some database D represented by the table below:

Joe	21	NYC	CIS	2.7
Mary	19	PHL	MATH	3.1
Eve	20	BOS	ENGL	3.4
Bob	20	...	...	4.0
...	...	...	...	...

The consumers whose data is in this database would naturally be worried about the release of sensitive parts of this data such as GPA. This worry is concerned with data security.

3.1 Machine Learning Application Model

The typical application of machine learning starts with a set of data such as the one above. Then, the data is fed into an algorithm, which then produces some output, whether it be statistics, a neural network, a modified database, product recommendations, etc.

3.2 Two Stages of the Model

This model can be broken up into two stages in regards to privacy: the first stage involves the data itself and the second stage involves both the algorithm and the output. For each stage, we are going to want different definitions of privacy. In this lecture, we are only concerned with the first stage. The ultimate goal of this first stage is to keep the data from the database "locked." That is, we want to prevent hackers from gaining access to the data. In other words, the goal is to prevent unwanted interference. This subset of privacy concerns is what Cryptography (crypto) deals with. Privacy in this stage is an issue that is relatively solved because very good algorithms, methods,

and notions of security of data already exist. Specifically, cryptographic, algorithmic protocols are very well understood. Yet of course, like with fairness, there is going to be tension between utility and privacy.

4 Keeping Data "Locked" (Cryptography)

The goal of cryptography is to encode data such that the encoding would be indistinguishable from a random string.

4.1 "One-time Pad"

"One-time Pad" is one method of encoding in Cryptography. Say we have a message we want to encode and say this message is 100 bits. We'll represent this original message as $a = a_1a_2...a_{99}a_{100}$. We want to produce a pad (key) with a length of 100 bits where each bit is randomly chosen. We'll represent this key as $b = b_1b_2...b_{99}b_{100}$. This pad is the key necessary to decipher a message. Now, to encrypt the message, we will convert $a_1a_2...a_{99}a_{100}$ and $b_1b_2...b_{99}b_{100}$ to $c = c_1c_2...c_{99}c_{100}$. To do so, we use the exclusive-or logical operation, denoted as $\bigoplus$. Every c_i in c will be converted like so: $c_i = a_i \bigoplus b_i = 0$ if $a_i = b_i$, or $c_i = 1$ if $a_i \neq b_i$. By doing this, regardless of what b_i is, $a_i \bigoplus b_i(c_i)$ will look like a random bit. Now, to decrypt c, and figure out a, all you need to do is exclusive-or c_i with b_i again: $(a \bigoplus b) \bigoplus b = a \bigoplus (b \bigoplus b)$. A big issue this method has, however, is that the key can only be used once since using it multiple times can lead to cracking the code. To demonstrate, say we are given $(x \bigoplus b)(y \bigoplus b)$. Performing the operation $(x \bigoplus b) \bigoplus (y \bigoplus b)$ gets you $x \bigoplus y$, which must be either 1 or 0. Besides this issue, there are also a few other drawbacks to this method including the password itself taking a lot of space, the need to have a secure location to come up with code and share the code, and time inefficiency of getting everyone to learn the password in pairs.

4.2 "RSA Cryptosystem"

The "RSA Cryptosystem" is another method of encoding in Cryptography. For example, let's say person A wants to send a social security number x_1, x_2, $x_3...x_m$, where each x_0 is at most 1K bits long to person B. The two people then get together and choose 2 2K-bit long prime numbers p q. Then they define N = p * q and person A sends another number e 1K bits long to person B. Person B sends x^e mod N and the keys are p and q. We then define p, q, and e as d, where we then assert $(x^e)^d$ mod N as the final RSA cryptosystem. The process of encryption and decryption here is exponentially efficient. One could say that an adversary could crack the code here by factoring N, but there is no fast, efficient algorithm for factoring. So, having the longer keys makes it harder for this adversary to crack the code.