The difference between privacy and security, and the relationship between them.

Since our topic is the **privacy** of genomic data, I’d first like to clarify the difference between privacy and security but also show they are related, because we may also talk about security.

Firstly, to be secure means to be free from threat or harm, but security as an a more general term can also refer to the methods used to be safe or protected. Privacy on the other hand is the ability to decide what is or isn’t shared with others. For an easy to understand analogy, **privacy is me deciding how much of my cake I want to share with you, security is me being able to defend my remaining slice from being taken.**

Now if you think about it, privacy depends on security, because if you aren’t secure then you don’t have the power to enforce your decisions. In other words, if you can take my remaining slice of cake from me, then my decision of how much I wanted to share was irrelevant.

This is why security is relevant to our discussions of privacy - if your security is at risk, your privacy is too. (1 MINUTE)

DNA databases & criminal investigations

So, I’ll be talking about the usage of DNA databases in criminal investigations.  
  
SLIDE

The main ethical questions here are: should police have access to genealogical databases for solving crime? And if so, should individual consent be required? Basically, is their access going to be a **breach of privacy**, and if so, **do the benefits justify this breach**?

In answering these questions, it’s necessary to first cover how and why police use these databases, and the associated benefits and ethical considerations.

SLIDE

The main reason police use genealogical databases is for solving cold cases. The way in which this is achieved is by firstly uploading a sample of the suspects DNA from the crime scene to an online genealogical database, most often GEDmatch. A long-range familial search, a fancy term for finding relatives, is performed, and from matches and other public records, a family tree can be built. Police then research the people in this tree to hone in on the most likely suspect. They then obtain DNA samples from the suspect and sometimes family members, either voluntarily, via a warrant, or via abandoned DNA – which is DNA you have left behind, in the hopes of finding a match. Using this method, GEDmatch alone has been used to make 59 cold case arrests.

SLIDE

Conversely, the same technique has been used to prove the innocence of suspects and even exonerate wrongfully convicted people. For example, an organisation called the innocence project used GEDmatch to exonerate Christopher Tapp, who spent 20 years behind bars for a rape and murder he did not commit. Tapp confessed to the crime in 1997, but the confession was coerced and false, which occurs more than you would think. This is a huge benefit considering exonerating innocent people is perhaps more important than convicting the guilty, and due to the uniquely identifying nature of DNA, it’s able to trump less substantial evidence that was used for wrongful conviction, so it’s really effective.

SLIDE

Furthermore, this technique can be used to identify previously unknown victims, not just criminals. For example, the DNA Doe Project (an organisation named after Jane and John Doe, pseudonyms for unknown victims) again used GEDmatch in 2018 to identify their first victim, Marcia Sossoman, who was a murder victim who went unidentified for 36 years. This is another clear benefit, in that it provides the much needed closure to the families of the victims. [include solved 11 more since on the slides]

SLIDE

Finally, you could even go as far as to say it prevents crime, as the chances of being caught are so high that it acts as a deterrent.

SLIDE

So, are these benefits worth the breach of privacy? Well, firstly, it’s worth noting that ancestry-based companies like 23andme and ancestry.com will only voluntarily give your data to police for **MAJOR** crimes or when compelled to via a warrant, which also indicates a major crime. Considering police are only interested in a small portion of the data that is linked to the suspect, the invasion of privacy is pretty small, and so it’s reasonable to argue **that the payoff is well worth it, considering the crimes being solved are especially heinous.**

SLIDE

Furthermore, sites like GEDmatch, which is the most popular genealogical database for police to use, allow you to opt in or out of police searches. This eliminates the breach of privacy aspect from the equation completely, **transforming the ethical dilemma into a non-ethical one**, where all parties’ interests are aligned. This indicates that consent should be used, as it can achieve the most desirable outcome and is perhaps the route all genealogical databases should take. The issue here is that a large percentage of users may not be bothered to log in and manually opt-in, which is what happened with GEDmatch, causing the number of accessible profiles to plummet from over a million, to less than 200,000, which significantly hinders the effectiveness of the database. The solution may be to opt users in by default, as opposed to out, which isn’t so bad when you consider that a survey by Guerrini et al found that 80% of surveyed individuals support police searches where the purpose is to solve violent crimes. Additionally, it still provides the option to opt-out, and it could be argued if you aren’t bothered to manually opt-out, then you don’t actually value your privacy as much as you say you do.

SLIDE

On the topic of GEDmatch, remember how we stated earlier that privacy depends on security? Well GEDmatch is actually a perfect example of this. Due to two SECURITY breaches in July of this year, all profiles settings were set to opt-in, thus removing the CHOICE from users (and hence eliminating privacy and turning the situation back into an ethical dilemma). This is important to note because whilst your privacy is a right, it’s not a guarantee, and so even if you opt-out, you still need to be cautious about the possibility of your data still being accessed.

SLIDE

You may have noticed earlier that I stated police often take abandoned DNA samples and upload them to databases. Whilst these have been immensely useful in catching criminals, it could be argued that this is an even larger invasion of privacy, especially in cases where they are uploading the DNA of innocent people, because in this case DNA isn’t being uploaded by the owning individuals themselves. It’s clear from our talk on dataveillance that users may have an expectation of privacy when uploading their data to companies themselves, such as when doing ancestry tests, but if police are doing it on their behalf, then their privacy has been entirely breached and this exposes them to the potential risks outside the realm of policing. It’s quite clear that you cannot expect your abandoned DNA to be private, you simply shed too much of it, but whether police should be allowed to further violate your privacy and upload it on your behalf is another question. Police should be very cautious about uploading a suspects DNA, because whilst it’s legal, it’s quite unethical if the ends don’t end up justifying the means i.e. if it doesn’t lead to an arrest.

SLIDE

Personally, I believe police are one of the best candidates for parties that have access to our genomic data, as the benefits outweigh the usually small breaches to privacy. Tell me what you think in the discussion later on!

END OF TALKING HERE

Some notable examples of criminals caught using these methods were the Golden State Killer, who was ultimately identified with tissue … This leads me onto the next ethical consideration. **Should police be able to sample and upload DNA you have left behind to these genealogical databases?**

the most famous of which was that of the Golden State Killer who was a serial rapist and murderer who terrorized California in the 70’s and 80’s but wasn’t caught until 2018. He was caught because a detective decided to upload DNA of the suspect taken from a crime scene to GEDmatch, a large online **public** DNA database. This database returned ~20 relatives, from which they constructed a family tree, identified the people behind these genetic profiles, and researched them until they were confident that they had found a suspect. Then they took a tissue from his trash to sequence the DNA on it and confirm he was indeed the criminal. This is a huge win for DNA use in criminal cold cases, and it’s not alone.

Also in 2018, John Miller was convicted for the kidnapping, rape, and murder of an 8 year old girl, April Tinsley, which occurred in 1988. Detectives similarly uploaded crime scene DNA to GEDmatch, generated a family tree, narrowed down the likely suspects, ultimately using a DNA sample from his trash to prove he was the perpetrator. ABC News <https://www.youtube.com/watch?v=qdSH00I-P90>

1997 Lorrie Ann Smith was murdered by

2001, Christine Franke was shot dead in her apartment, crime scene DNA was again used in 2018 to find the killer. Detective partnered with a genealogist who used GEDmatch to reverse engineer a family tree. They ended up getting a voluntary sample from who they **theorised may be the mother of the suspect, which was proven to be true.** The son was arrested after DNA taken from a cigarette butt he threw on the ground matched him to the crime scene. <https://www.youtube.com/watch?v=CigubAVY9MM>

This raises another ethical issue – **do you still have rights over your abandoned DNA?** Should police or others be able to sample it and submit it to genealogical databases? Well, even if they aren’t allowed to, they can just get a warrant to anyway.

Further Ethical concerns;

1. Inadvertently turning in your family
   1. You might inadvertently turn in a family member by doing an ancestry DNA test – too bad?
   2. A criminal who has never given their DNA may be identifiable – too bad?
   3. In all cases, this boils down to: do criminals deserve to be punished for their crimes? Obviously, yes.
2. False positives
   1. If you don’t use DNA then you may be relying on more subjective evidence and more people might be wrongfully convicted than if you were to use DNA. The error rate is so low that it is better to use it than to not use it, as long as this risk of false positive is acknowledged and considered when convicting it is fine.
3. The government/police having your DNA in general. They can do anything they want with it in the future. Who knows what will be possible with DNA
   1. I think this is the most legitimate ethical claim.

Conclusion/answer

Yes, they should have access as the pros outweigh the cons. However, consent should be included for opt-in databases (such as with ancestral tracing).

Points to get in somewhere..

* this is another ethical issue: is DNA you leave behind still yours? Should people/police be able to take that and sequence it? Is this an invasion of privacy?
* Need to mention the difference between opt-in databases like ancestry.com/23andme/GEDmatch vs non-opt-in ones like criminal databases (find the name of that American one)