Ethical dilemmas and data sharing in genetic genealogy

John Cleary, Heriot-Watt University

- Surveys of genealogists and the wider public appear to show overwhelming support for law enforcement use of genealogical databases (see Graphs below - Fig. 7 and Fig. 10, from Gleeson, 2018)
- There is a need for qualitative understanding of the motivations and reasons underlying these views
- Is there a disconnect between the views of the above groups and ‘opinion leaders’ in the field?

METHODS

- Focus group discussions with active genealogists (professional self-employed or active in undertaking work for others)
- Expert interview series with (1) sample of above; (2) opinion formers, educators, project leaders in genetic genealogy; (3) specialists in forensic and legal issues
- From the Glasgow focus group, 2019:

I would agree with that, because basically what we use the sites for is we upload DNA, usually ours or family members, and we are looking for matches. In my view that’s what the police did, they uploaded a DNA sample and they were looking for matches into a family. So in my view they were doing the same as we are doing.

I think for this woman’s family it gave them closure and I think that’s a positive and I think that’s what it’s used for then I think that’s a good idea. I guess if there are police forces where that is cooperation, then it mightn’t always be used for good.

Like in health there’s only privacy to the extent that if someone commits an offence, you have to give that information to the police. So it’s no different from that case.

That expertise can be used for good or bad so it needs to be part of an ethical strategy.

I would hope there would be some kind of contract between the security services and that project, so they are not giving you this data, here is what we would like you to do with it, so it was cooperation under some kind of contract.

In essence an amateur group might not, you know there might not be any data entry to this group. We don’t know who might be involved, it could be anyone. Whereas if it’s a professional group there are safeguards.

ConsenSUS & RE-PURPOSING

- Members of the databases had not given prior informed consent for law enforcement use
- Can searching for “Jane/John Does” (persons unknown) be judged as a “genealogical use” compared to uses accepted by community?
- Does identifying criminals constitute a repurposing of the databases away from uses consented to?
- Does post hoc re-drawing of Terms of Service mean consent is received? Are opt-out policies sufficient to protect users?

PRIVACY V. SOCIAL GOOD

- Private data on enthusiasts in genealogy databases is accessible to agents of law enforcement: networks of possible relatives (“matches”); linked family trees; contact details
- Chromosome browsers may allow DNA data to be deduced
- Sacrifice of privacy may carry social justification for crimes of extreme violence?
- Is there risk of “mission creep” to non-violent offences – and does this matter? If a line should be drawn – where?

RECIPIROCY

- Will law enforcement agents be able to access more information about matches than individual members who uploaded their own data?
- Is it acceptable/advisable for those with strong privacy concerns to hide their data using ‘research status’ or ‘no-matching’?
- Does this harm the overall enterprise since it is based upon data-sharing? Is it ethical to receive information about other members while hiding one’s own?

OVERSIGHT & PROCESS

- Is there a risk of sensitive information on targets, victims or investigations being leaked through weakly controlled access?
- Are individuals matching crime scene samples safe from having their identities revealed? Are they at risk of retribution?
- How is the ability or reliability of the caseworkers assessed?
- Are procedures for contracting, regulation and audit sufficient to prevent abuses of data?