THE SPECTRE OF ANONYMITY

Seda Gürses

In dystopian debates on digital privacy, it is suggested that privacy can only be protected if we hide our personal information or practice control over it. In my paper I will look at the strengths and weaknesses of anonymity in each case, both as a technology as well as a strategy. I will also delve into its relationship to control, meaning how it evades and replaces different forms of control.

Anonymity is a powerful concept and strategy. It supersedes concepts such as authorship and origin, and manifests itself in our songs, poems, oral histories, urban legends, conspiracy theories, chain mails… For centuries, communities have used anonymity to articulate their collective voices. Anonymously produced statements or artefacts have expressed the cultural practices, beliefs and norms of the past, while creating a space in which to collectively build the future.

Anonymity allows the individual to melt into a body of many, to become a pluralistic one, for which the act of communicating a message is more important than the distinction of individual participation, be it at a demonstration or a football match. Yet, the seemingly unbreakable bond is fragile, since participation in the anonymous is fluid and is organized in a distributed manner. The anonymous perseveres only as long as the common line is held, hence at any point it may experience dissonance and simply dissipate. It is hence the volition of its participants that distinguishes anonymous groups from other types of collective bodies.

Anonymity is a means, never an end in itself, and can be utilized in unexpected ways. For example, in centrally organised forms of anonymity, e.g., military, corporation, participation in the anonymous is mandatory, individual actions are heavily controlled. The objective is still to protect, though the ones being protected are not necessarily the participating individuals but the existing power hierarchies.

The power of anonymity in communications has long been recognised by computer scientists and hackers. Anonymity is hence also a strategy on the Internet. So I ask, how is anonymity implemented, why, and by whom? What are its strengths and limitations?

‘Anonymous communications’ technologies like TOR, strip messages of any information that could be used to trace them back to their senders, so that a set of individual communication partners are not distinguishable. Observers cannot determine who is communicating with whom, so that individuals are protected against any negative repercussions resulting from such disclosure.

The architecture of the Internet makes it plausible to track the data bodies the users of the Internet leave behind, approximating all actions to their individual authors in physical space and time. These data bodies are open to scrutiny, dissection and re-use by collecting parties. By masking the origin, anonymous communications channels protect the individuals who authored these data bodies.

Despite the diversity of the groups and communities using anonymous communications, such technologies are usually cast in a negative light in policy papers and in the media. Anonymous communication

infrastructures are seen as providing channels for criminal activity or enabling deviant behaviour. But perhaps what bothers authorities most is not the fact of anonymity as such, but rather the user base and the distributed organization it relies on. After all it is obvious that data miners and regulators are keenly interested in systems that generate another type of anonymity, database anonymisation, a technique that is instrumental to the growing data economy.

The ideology behind the current data-driven economic hype suggests that the data collected will make the behaviour of populations more transparent, easier to organise, control and predict. Massive datasets are expected to reveal ways of improving the efficiency of markets and systems of governance, by applying statistical analysis methods to these datasets to infer knowledge. According to behavioural advertisers and service providers, these datasets will become 'placeholders' for understanding populations and allowing organisations to provide them with refined individualised services. In the process, elaborate statistical inferences replace 'subjective' discussions, reflections or processes about societal needs and concerns. The data comes to speak for itself.

However, collecting and processing such massive amounts of data is historically linked with a serious privacy problem. This is where database anonymisation provides a protection. The database can be manipulated in such a way that the link between any data body included in the dataset and its individual 'author' is concealed, while the usefulness of the dataset as a whole is preserved. If this is somehow guaranteed, then the dataset is declared 'anonymised'. Inferences can be made from the dataset as a whole, while ideally no individual participant can be targeted. This approach is endorsed not only by data miners, but also by regulators. The EU Data Protection Directive [1] includes a clause that frees anonymised datasets from regulation.

Once the link between the original author(s) and the message is broken and the message is released, it is likely to be subverted and reclaimed by others. This is one of the charms of the anonymous message: any individual or group can claim it as their own. But when a group subverts the message to negate all other linkages and continuities, monopolising the interpretation of the message's senders, destination and content, the relationship between 'the anonymous' and the message can get lost.

An example of this is given by Adela Peeva in her documentary film "Whose is this song?", [2] where she searches across the Balkans for the origins of an anonymous folk song. In each country or region she visits the song changes, becoming a love song, a song of piety, even a war song. Each variation comes with conflicting claims about the song's 'true' origins, all of which attempt to separate it from its nomadic past. The song is invariably re-shaped to uphold the local collective memory, as well as the community's future identity, in mostly not-so-subtle stereotypes: young Turks, amorous Greeks, proud Albanians, pious Bosnians, debauch Serbs, superstitious Roma, unflinching Bulgarians…

The film captures the dilemma associated with any anonymous action or artefact. Anonymity allows the articulation of a collective message. The message travels, free from the burdens of origin or authorship. However, this freedom is limited when a specific group claims the message as its own, and bends the message to suit its own interpretation of the past or future. The anonymous message can then boomerang to hit its collective authors: the hijacking of popular uprisings by a small group establishing its power, the re-writing of folk songs into chauvinistic hymns, or using anonymous actions as a pretext to introduce draconian security measures, are all examples of such de-contextualised anonymous messages.

In the data economy, the anonymised dataset becomes a digital mirror of the population's activities and tendencies. Organisations that hold a monopoly on these datasets assert their own categories of (un)desirable activities, in order to improve their markets and forms of governance. Since such datasets are anonymised and cannot be linked to individuals, privacy is supposedly intact (though anonymisation techniques provide no formal guarantees) and so the general population is not expected to question the ways in which the anonymised data is used.

We have seen how anonymity can be used to collectively protect individuals against Internet surveillance. But we must also recognise how similar strategies are being used to create discrete, decontextualised (yet linked) datasets that are essential to the data economy. We now have huge databases of 'friends' who rate, tweak and 'like' information which can then be used to guess our interests, desires, passions and weaknesses. The goal of the anonymisation of these databases is not to protect individuals, but to make it impossible for them to understand, scrutinise or question the ways in which these datasets are being used. We must cherish anonymity as a strategy for protecting individuals online, while rejecting its reincarnation as a tool to separate us from datasets being used to manage our lives.

Anonymity will always remain a powerful means of achieving political objectives and spreading collective messages. However, especially in political contexts, the vulnerability of the anonymous means that multiple strategies should be used to create a continuum of anonymously initiated activities. This includes making political statements that are explicit and precise, sometimes anonymously, sometimes not.

References and Notes:

1. European Union (1995). Data Protection Directive (Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data). Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML (accessed September 2011).

2. Whose is this song?, dir. Adela Peeva, Copyright 2003, Adela Peeva.