Social Palimpsests - clouding the lens of the personal panopticon

*Dave Murray-Rust, Max van Kleek, Laura Dragan, Nigel Shadbolt*

The use of personal data has incredible potential to benefit both society and individuals, through increased understanding of behaviour, communication and support for emerging forms of socialisation and connectedness. However, there are risks associated with disclosing personal information, and present systems show a systematic asymmetry between the subjects of the data and those who control and manage the way that data is propagated and used. In this chapter, we explore a set of techniques for ameliorating the tension between the desire for the benefits of sharing and a distrust of those with whom we share our data.

Increasingly, in order to utilise services, we must provide our data to third parties. This ranges from mobile phone numbers being required for Yahoo accounts, to location data being shared with Foursquare or Grindr, to the NHS adding personal health information to centralised databases. We call this *fiat data* - an organisation uses its position to demand (by fiat) the disclosure of certain information in return for use of its services. In some cases, this is a necessary requirement for the service to be worthwhile, but in many cases it represents an attempt by the organisation to create a monetizable product from its users.

Sharing data, by definition, is the entrusting of other parties with information; this necessarily involves relinquishing control over how it is subsequently handled and disseminated. However, data is persistent, while people and contexts change. A government may decide to share previously confidential data, as in the case of the recent care.data fiasco in the UK; a company can be bought and its assets acquired–the purchase of Moves by Facebook raised issues around the terms and conditions of data handling companies; and even without malice accidents can expose vast swathes of personal data, or court proceedings may force private communications to become public - the Enron emails still represent the largest publicly available corpus of private emails.

A natural part of online life is the ability to tailor the persona we present to different communities and contexts. An individual may want to disclose certain things to their professional colleagues, while presenting differently to friends and family or non-mainstream friend groups. Sharing certain personal data is a barrier to this, as its basis in physical fact provides multiple opportunities for joining up otherwise separate databases. Most, if not all, social interactions involve both strategic omissions and various kinds of lies and non-truths to manage the myriad conflicting social demands placed upon us. The *lie maintenance* required to avoid discovery may be trivial (“sorry, I’m hungry, have to go!”) but may become significantly more complicated as lies extend over time, and become woven into the social fabric.

Personal data stores (PDS) represent a partial solution to issue of presentation: having trusted, user controlled repositories for data enables a more user-centric approach to management of *capta*–those data which we choose to take and preserve. Bridges can then be built between personal data stores and the rest of the world in order to support the connected, networked interactions which users now expect. If these bridges simply share the data, even in a controlled manner, nothing has been gained; hence the bridges become conduits for manipulating truth and constructing falsehoods. As personal data stores accumulate more real-time contextual data about the individual, as well as about the individual’s social connections, PDSes can provide support for the often stressful and mentally burdensome task of lie maintenance, for example: *i)* identifying when a person’s real activities or whereabouts contradict a lie, and might be discovered; *ii)* identifying indirect social channels that could expose a lie (e.g. through friends of friends); *iii)* suggesting appropriate lies to use which are least likely to be detected; *iv)* suggesting individuals to lie to to support lie maintenance (e.g. friends of the person being lied to).

Sharing is a crude mechanism. Once data has been shared, the originator can no longer exert control over it, and must rely on the behaviour of the recipient, which as noted may fail to meet user expectations. Validation, however is a more subtle tool: if a user’s personal dataset can be made sufficiently questionable as to be useless on its own, then locus of control shifts to the user choosing to validate parts of the dataset, which can be performed in a more nuanced, contextualised manner. If a user is the final arbiter of trust, they can decide to i) sign parts of their record, so that it is verified public fact; ii) co-sign it with another entity, so either can verify it but not anyone else; iii) verify it through an anonymous channel, so that the entity to whom they provide verification cannot propagate the claim further. This verification can be carried out entirely separately from the datastore itself, allowing for the presentation of different datasets as valid in different contexts, as well as unorthodox methods such as using the Bitcoin blockchain to notarise datasets, so that they can be verified in the future without revealing them as true at the time.

How can data be made sufficiently questionable? While there are many potential techniques we focus on ways to construct lies–or more charitably *fictions*–about ourselves such that an outside observer cannot be sure which values are true. The four main techniques we examine are:

* *noise injection*, where some form of noise or error is systematically introduced into the shared data;
* *noise flooding*, where huge amounts of random data are added to the actual signal;
* *unreliable narration*, where segments of the data are replaced with plausible, coherent but untrue narratives;
* *palimpsestification*, where a sheaf of plausible but incompatible histories are continually generated, so the true history is not immediately discernible.

Working in this manner, the questions become: which kind of unreliability is appropriate to engage with a particular service? how can we find an optimal balance between preserving plausible deniability and providing enough truth to benefit from the engagement? and how can we construct these fictions in a socially-connected world, which may accidentally “ground truth” us at inopportune moments.

This final question relates to the novelty of our thesis; while the ideas around steganography and lies are not new, what is new is the manner in which our social linkages both help and hinder our storytelling. There are opportunities for collusion and federated lying; for groups to work to expose a person’s actions; and for a chance encounter in a coffee shop to unravel a whole saga of fabrications. We hence ask the question: how can we maintain control over the quantum superposition of our personal data states, and choose when and how the wave function collapses.