Social Palimpsests - clouding the lens of the personal panopticon

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

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.

# 

# 

# Abstract

# Introduction

## The collection and use of personal data

* more and more tracking going on
* hard to avoid

## Personal data stores and lifelogging

* *sousveillance* - bottom up recording of stuff
* intimate, first-person datasets
* long term records - generally, we don’t understand the implications of collecting and keeping all this data

## ‘Fiat data’ and the information panopticon

* much of this data collection is enforced to allow you to use services
* e.g. Facebook etc.
* but more insidiously governments etc. “national X databases”

## Impossibility of Controlling Spread

* We can’t control the spread of data
* Half of it is by organisations we don’t even know are collecting/tracking it
* Once someone has it, there’s no (technical) way to enforce that they delete it or refrain from disseminating it.
* Fundamental issue - essentially a parallel to DRM; would need to have sandboxed/trusted areas on everyone’s device (even Snapchat cant manage it when they control both ends)
* Even when we try to control our data **our friends are idiots**. You can avoid using gmail so they can’t read your mail, but you might have to work with people using it; can’t stay off their servers

## Validation instead of control

* We can’t get to control who sees “our” data
* But if we can introduce doubt that it really is ours, then we can control which bits we own up to
* And validation is more subtle than sending data

# Palimpsestification

## PDSs - more than just a bucket of bits

* control how data is shared, who can see what
* build in intelligence on top of the data - applications, connections, communication etc.
* will increasingly function as gatekeepers between us and the outside world

## Scenarios for fuzzification

(using location checkins as an example for now)

### Adding noise

* PDS sits between you and the data collector
* Misrepresents your location - instead of checking in where you are, can check you in somewhere nearby
* Because it’s clever, it can do this systematically - e.g. always finding a greasy spoon rather than the gourmet coffee place you’re really in
* At the same time, it remembers your real location, so you can use it

### Multiplicity

* Make lots of checkins - more than a real person could - including the real ones
* Remember which ones are real
* Can provide corrected (or putatively corrected) versions if you want

### Presenting Fictions

* Create alternative possibilities, which are plausible

### Federated Lying

* Gang up with friends to produce good stories

### Account Sharing

* Create multiple amazon accounts and use them to buy different stuff to skew the profiles

## Why Verification is better than sharing

* When we share, people have the data
* If they have to prove it is valid, however, things change
* We can sign it - then it’s public record
* We can co-sign it, so that only that person can also verify it’s true (although they can share that knowledge)
* We can just say it’s true (using some anonymity preserving channel), and then they can’t ever prove that we said it’s true
* We can notarise bits of data in the bitcoin block chain to give timestamps etc.
* etc.

# Discussion

* How do these examples work with other data? e.g.
  + medical records
  + government collected stuff?
  + things that should be a single time series?
  + purchase histories
* Is it OK to lie to get services? What about to your friends?
* Does it scale? What happens when FB blocks it?
* Do you also need to disavow/burn bits of data?
* Why is this new? It’s the social, automatable aspects; having access to our whole lives to construct plausible, long running inventions; using friends to help create alibis;
* Maintaining distrust - how to make sure that noone believes your data in general, and specifically if a third party tries to assert bits of your data without your consent.

# Useful bits:

## Mail sent to Kieron

The Social Palimpsest: anonymity through verification and personal data stores.

In a <post Snowden ;) > digital networked world, sharing any data means there is a strongly nonzero chance that it becomes publicly available/widely shared/owned by facebook/known by NSA etc. Given that we want to be able to use our data, and we don't want to completely loose control of it, we need an approach that puts people back in control but which is compatible with widespread visibility.

To make this happen, we ensure that everyone emits a stream of junk data - e.g. erroneous location traces - into which their real data is mixed. Control of data then becomes control of validation - do I agree that these data points are really mine. Validation is more finely grained than sharing - I can validate by signing it, in which case it becomes public record; or we can co-sign, so that only the requester can prove that I signed the data; or I can validate by nods/winks/anonymous Tor links/etc, in which case the requester cannot prove that I validated the data to anyone else.

And the personal data store is where you do this - so you put your real stuff in your PDS, and allow it to send out a million different made up stories about what you're doing. People then contact your PDS to discover which of the ephemeral micropersonae are 'true'.

I think this gives us an interesting twist on how to control personal data (although I'm sure it's not a new idea in general).

Alongside this, I'd like to introduce the notion of "fiat data", a heroically tenuous analogy with fiat currency. Fiat currency (which is most of them, now that noone's on the gold standard) derives it's value from being the official currency of a government (ultimately from being the currency in which tax is demanded). Cryptocurrencies etc. derive their value purely through belief (with a nod to artificial scarcity).

So the analogy is that "fiat data" is when in order to use a service, you have to put your data into the format/silo/control of an organisation; the database gains it's value/content because the organisation demands taxes in return for services. PDS's work more like cryptocurrencies - the network of datastores derives value from everyone individually having decided that it's worth putting data in.

Notes from eMax

Most, if not all social interactions today involve the strategic and natural deployment of various kinds of lies and non-truths, in order to manage the many and myriad kinds of social social demands we have during our daily social interactions. Such lies can range from the small so-called ‘butler lies’ [Hancock et al.] that arise when, for example, we use an excuse to gracefully exit a conversation, or courteously decline an invitation, to more moderate-sized lies that people deploy simply to avoid having to tell a person explicitly that they do not like their company, their advances, or their behaviour.

One of the tricky things about lying is the need to maintain the lie after it is made, to prevent the lie from being discovered. This *lie maintenance* may be trivial (“sorry, I’m hungry, have to go!”) but may become significantly more complicated as a lie is longer, involve unusual situations or circumstances, or multiple parties. Lie maintenance primarily involves ensuring that recipients of lies do not discover information that contradicts the lie, such as the truth, or another lie, either by behaving in a way that is consistent with the lie or using more lies (strategic cover-up).

While most of these lies are personally deployed and executed, one of the most challenges roles of personal assistants (PA) may be to manage (and maintain) another person’s lies, namely those of the person they work for. In the future, as personal data stores accumulate more real-time contextual data about the individual, as well as about the individual’s social connections, it may become feasible for PDSes to provide PA-like support for the often stressful and mentally burdensome task of lie maintenance. We imagine lie maintenance will provide the following kinds of activities:

- identifying contextual lie conflict disclosure - when a person’s real activities or whereabouts contradict a lie, and might be discovered

- identifying indirect social channels that could expose a lie (e.g. through friends of freinds)

- suggesting appropriate lies to use which are least likely to be detected

- suggesting individuals to lie to to support lie maintenance (e.g. friends of the person being lied to)