

# Transparency Enhancing Technologies to Make Security Protocols Work for Humans

Alexander Hicks and Steven J. Murdoch

# Bates & Ors v Post Office Ltd

- Many UK Post Offices are not run by Post Office Limited but by self-employed agents (subpostmasters) acting on behalf of Post Office Limited (POL)
- Products, commercial agreements, and accounting computer system all developed by POL with very limited discretion of the subpostmasters
- If the accounting computer system (Horizon) records a shortfall then subpostmasters are personally liable for making it good
- Claimants contend that Horizon has incorrectly recorded shortfalls due to bugs



# I'm not a subpostmaster, why should I care?

- Dispute running since 2000's and in the meantime subpostmasters have been bankrupted, jailed, and died while still waiting resolution
- One of very few cases about alleged failures in complex computer systems which has made it to trial and been adequately resourced to get to the bottom of both legal and technical issues
- Post Office is an “arms-length” government body, bankrolled by the taxpayer, and considers the litigation an “existential threat”
- Subpostmasters are part of a Group Litigation Order and backed by billion dollar investment fund – Therium



# What do I mean by adequately resourced?

- Both sides spent £10 million between themselves before the trial even started (including legal costs, expert witnesses and “shadow experts”)
- Multiple QC’s for each side
- Most recently Lord Grabiner acted for Post Office – Master of Clare College and charges £3,000 per hour for his advice
- Compare to disputes over Chip and PIN which maybe involved thousands of pounds



# Civil disputes decided on balance of probability based on evidence presented

$$\underbrace{\frac{P(\textit{liable} \mid \textit{evidence})}{P(\neg\textit{liable} \mid \textit{evidence})}}_{\text{posterior odds}} = \underbrace{\frac{P(\textit{liable})}{P(\neg\textit{liable})}}_{\text{prior odds}} \times \underbrace{\frac{P(\textit{evidence} \mid \textit{liable})}{P(\textit{evidence} \mid \neg\textit{liable})}}_{\text{likelihood ratio}}$$

Is it more likely than not,  
given the evidence, that the  
claimant is liable

Before you saw the  
evidence, is it more likely  
than not that the  
claimant is liable

What is the relative  
likelihood of the  
evidence occurring if the  
claimant is liable versus  
them not being liable

# Application is naturally circular

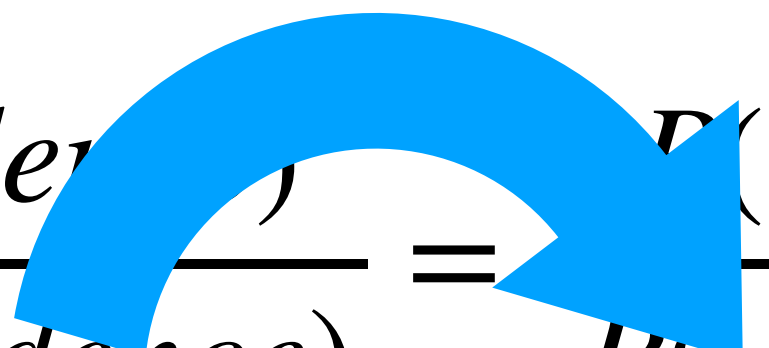
Posterior odds from previous disputes becomes prior odds for next



$$\underbrace{\frac{P(liable | evidence)}{P(\neg liable | evidence)}}_{\text{posterior odds}} = \underbrace{\frac{P(liable)}{P(\neg liable)}}_{\text{prior odds}} \times \underbrace{\frac{P(evidence | liable)}{P(evidence | \neg liable)}}_{\text{likelihood ratio}}$$

# This sucks for claimants

- Very unlikely scenarios (like cryptography flaws) disappear
- Likelihood ratio doesn't help when both computer error and human error (or fraud) by the claimant are explanations for the evidence
- Posterior hinges on prior odds and human error (and fraud) is obviously something that can and does happen
- Decision of human error then becomes the new (more certain) prior

$$\underbrace{\frac{P(\text{liable} | \text{evidence})}{P(\neg \text{liable} | \text{evidence})}}_{\text{posterior odds}} = \underbrace{\frac{P(\text{liable})}{P(\neg \text{liable})}}_{\text{prior odds}}$$


# Protocol proofs don't help

$$\underbrace{\frac{P(\textit{liable} \mid \textit{evidence})}{P(\neg\textit{liable} \mid \textit{evidence})}}_{\text{posterior odds}} = \underbrace{\frac{P(\textit{liable})}{P(\neg\textit{liable})}}_{\text{prior odds}} \times \underbrace{\frac{P(\textit{evidence} \mid \textit{liable})}{P(\textit{evidence} \mid \neg\textit{liable})}}_{\text{likelihood ratio}}$$



Reducing (already low) likelihood of protocol flaws just affects part of likelihood ratio that disappeared anyway



**Don't focus on where certainty can be inserted,  
but which has no effect**

“far better an approximate answer to the right question, which is often vague, than an exact answer to the wrong question, which can always be made precise”

— John Tukey (1962)

# Group litigation / class action

- Change meaning of prior odds from “the claimant erred” to “many claimants erred”, which assuming independence, can exponentially decrease human error likelihood
- One reason the Post Office trial is so interesting, with 500+ claimants

$$\underbrace{\frac{P(\textit{liable} | \textit{evidence})}{P(\neg\textit{liable} | \textit{evidence})}}_{\text{posterior odds}} = \underbrace{\frac{P(\textit{liable})}{P(\neg\textit{liable})}}_{\text{prior odds}} \times \underbrace{\frac{P(\textit{evidence} | \textit{liable})}{P(\textit{evidence} | \neg\textit{liable})}}_{\text{likelihood ratio}}$$

# Transparency

- Reduce likelihood of evidence being consistent with human error when that did not happen
- Multiple redundant, simple, and cryptographically assured audit systems to establish what actually happened
  - Interestingly Horizon was said to have a log of keystrokes (Credence) but in reality it seems less useful than was claimed
  - Legacy Horizon was asynchronous so nodes independently logged
- VAMS, designed for logging access to personal data by law enforcement or health applications, could apply here
  - Privacy features could reduce resistance to disclosing sensitive data

# Discussion – techniques depend on whether goal is better systems or better dispute resolution

- When the person designing the system is responsible for its failures, focus engineering resources on where it has most value
- Where third-parties may become liable system design should be forced to optimise for effective dispute resolution
- These goals may not necessarily be in conflict (other than for engineering resources) but they are not the same
- Courts are limited by the law, and so policy changes may be needed