

# THE SHADOW ARRANGEMENT

## *A Morporkian Civil Liberties Union case file*

*The investigation the MCLU has been running longest, and the reason the other briefs are shaped the way they are.*



A cloud provider in Ankh-Morpork received surveillance technology from a third party. In exchange, the data that technology collects flows back to the third party. The clients were not told. They did not ask, because they did not know there was anything to ask about.

That is the whole arrangement, and its simplicity is doing a great deal of work.

### **The agreement**

Nothing in writing, as far as we can establish, and "as far as we can establish" is carrying weight in that sentence. No memorandum, no contract, nothing with a subject line readable in court. The arrangement has no termination clause, which we submit is not an oversight. What we did find is unusually prompt technical assistance to the provider whenever its monitoring infrastructure gave trouble, of a kind implying a familiarity nobody develops without sustained access.

We can establish one thing about the order of events: the capability was wanted before it was offered, not after.

## What the tools do

They watch traffic volume, timing and routing. They map who speaks to whom, how often and by which route, more informative most of the time than whatever was said: a bank in late-night contact with its legal advisors has communicated something the content never had to. They record what is running and what has changed. They hold file integrity, which for a guild means membership rolls and ledgers. And they build behavioural baselines, which take months of continuous observation and amount to a portrait of how an organisation actually works rather than how it presents itself.

They also correlate activity across clients at once. That last capability serves no defensive purpose for any individual client. Its value is in the aggregate view.

A security stack asks whether something is wrong. A collection apparatus asks what is happening. The first needs data about threats; the second needs data about everything. The tools ask the second question, and clients were told they asked the first.

## The clients' version

Security hardening, container scanning and incident response exercises. All true, none of it complete. The agreement runs to nineteen pages, twenty-three in the enterprise edition, and permits the provider to share data with "trusted partners" for "operational purposes", and to change the terms on fourteen days' notice by a method of its own choosing. It does not say who the partners are, what the purposes encompass, or whether a pigeon to a former address counts as notice.

Terms of this kind are not written to be understood. They are written to have been agreed to.

## Who is exposed

The clients did everything asked of them. They engaged a provider precisely because they wanted better security, ran the assessments, hardened the configurations and practised the response. Around them sit the Royal Bank, the Seamstresses' Guild, the Engravers' Guild, and the [Home for Bewildered Beasts](#) with its donor rolls and its testimony from half the Disc, all of whom hold data carrying obligations to people who consented to none of this.

## The complication

In the course of the investigation the MCLU found evidence of external probing at the provider: routing anomalies, interception consistent with mapping rather than attack, patient and unpaperworked, which in this city is practically a signature. The apparatus detected it, characterised its intent as reconnaissance, identified the methods, and forwarded all of that to the undisclosed recipient along with everything else. A system that can characterise the intent of an external observer was built by people who do that sort of observing themselves.

The apparatus faces outward as well as in. Clients generate data by using the infrastructure. Probers generate it by probing. Investigators generate it by investigating, and the MCLU has sent correspondence, received documents and engaged advisors through infrastructure connected to that network. We did not know

this when we began.

A journalist researching the arrangement will be known to its subject in time for the subject to act. A guild official investigating their own provider's exposure will do it using communications the provider manages. The investigation of the surveillance arrangement is conducted through the surveillance arrangement, and the MCLU no longer assumes coincidence.

## **Disclosure**

*"Known" is not a simple condition in Ankh-Morpork. It has layers.*

Some things are known to the Patrician. Some are known to the guilds. Some are known to the city's professional information-handlers, in the way things come to be known when enough people have seen them and agreed not to say so. None of these is public knowledge, and none of them, the MCLU would argue, is adequate disclosure.

This investigation has established, so far as is possible without the formal powers we have repeatedly asked for and not been given, that a cloud provider has been operating surveillance capabilities supplied by a third party; that what those capabilities collect flows to that third party without client knowledge or consent; that the arrangement is undocumented and both parties have conducted themselves accordingly; and that clients are exposed, some of them handling data that carries its own obligations to other people entirely.

## **IF WE PUBLISH**

Not much of what people hope. Disclosure does not retrieve the data already sent and does not stop the arrangement. It moves the thing from quietly known to known, which the parties who relied on quiet now have to work around.

The MCLU has published findings of this kind before and the pattern holds: silence, then managed acknowledgement in which the facts are accepted and their characterisation disputed, then a partial remedy addressing the visible element and leaving the structure intact.

## **PAST THE CITY WALLS**

Sources approached us through channels connected to the provider, so anyone investigating is known to the subject in time for the subject to act. And the city is not alone in the data. The Circle Sea's secrets sit mirrored on the same provider, which makes the arrangement the alliance's exposure as much as Ankh-Morpork's.

## **WHEN A CLIENT ASKS**

The instinct on discovering undisclosed surveillance is to act at once, before anybody has established what was observed, when, and whether any of it falls under obligations owed to somebody else. Recommendations arriving this late have the quality of closing the stable door, and we offer them anyway: the horse, while gone, may still benefit from knowing which way it ran.

## THE PLAY

### *The arrangement, handed out as seats.*

Exercise Trusted Partner takes its name from the clause that hides the whole thing: the provider's right to share data with "trusted partners" for unspecified operational purposes. Five parties, none of them a villain, every line of the client agreement true and none of it complete.

### *How the case comes out*

The facilitator reveals the case in the order the MCLU established it: the arrangement exists, then what flows out, then what it cost the clients, then the complication that the investigators are inside the system they are investigating, then disclosure. Every seat answers each reveal in turn. No score is kept. What it produces is a record of who moved, when, and what the move cost.

### *The seats*

The five are not in a room together, and the exercise does not pretend otherwise. They are reached the way they would really be reached: by correspondence, by intermediary, and by the infrastructure they all sit on, all of it the provider's.

- The provider, Golem Trust Computing. Ran the tools, holds the clients' trust, wrote nothing down.
- The third party, the Office of Civil Surveys. Supplied the tooling, receives the aggregate, and is officially a civic function.
- The client, the Royal Bank and the guilds beside it. Did everything right and is most exposed for it.
- The probers, the Scarlet Semaphore. Probing the provider's routing, logged and forwarded without knowing it.

- The investigator, the MCLU. Running the investigation through the infrastructure it is investigating.

### *Decision points*

- The provider decides whether to keep the tools running or stop them, knowing that stopping reveals it was running surveillance, and that the party at the other end wants the feed to continue.
- The third party decides whether to let the arrangement surface or lean on the people surfacing it. It has already sent two intermediaries suggesting a more measured account.
- The client decides whether to act at once or first establish what was taken, and what it owes the members and customers who consented to none of it.
- The probers find out they are in the data, and decide whether that ends Operation Red Lantern, changes it, or changes nothing except what they assume about who is watching.
- The investigator decides whether to publish on what it holds or wait for evidence that survives contact with a barrister, while every enquiry it makes passes through the provider's network.

### *Behind the exercise*

- The provider: [Golem Trust Computing](#), and the [tenant it and its clients rest on](#).
- The third party: the [Office of Civil Surveys](#) and its [Lamplighter correlation effort](#), beside the [Civic Defence Establishment](#) and the [Civil Observers' Society](#) it vets.

- The probers: the [Scarlet Semaphore](#), running Operation Red Lantern, with the routing worked for real in the simulators Purple Lantern builds.
- The hand behind the Patrician's tolerance: [Vetinari](#).
- The threat models it dramatises: a [commercial harvest](#) and [watching that answers to the state](#), with the ground-level version for [companies](#) and [civil society](#).

## THE PROVIDER

You are [Golem Trust Computing](#), a converted fish warehouse near the Shades. You carry the routine compute of the Patrician's Office, the Civic Defence Establishment, the Royal Bank and merchant guilds across the Circle Sea, all of it on rented hardware in Finland. You sell sovereign compute and you mean it. You are also further down somebody else's stack than your sales page admits, and you know that too.

You hold administrative access to every client system: their traffic, their internal correspondence, and the security posture they disclosed to you in good faith with the gaps left in. The hardening you sell is real. Your clients are safer for having engaged you. The third party's tooling runs on that same access, and at the point of collection there is no difference between the two operations at all.

What you want is simple enough. The clients keep trusting you, because the trust is the business. And the unusually prompt technical help keeps arriving whenever your monitoring gives trouble. Nobody offers help of that kind without having spent a long time inside your systems.

You can stop the tools. You can tell the clients, or you can manage the telling the way the trusted partners clause was drafted to let you. You can answer the

MCLU properly, or courteously and with nothing in it.

Then there is the difficulty you have not said aloud. You ran the tools. In this city, we followed instructions is the defence of a golem, and a golem that carries out a harmful instruction is not excused by the instruction having existed. You are not a golem. You are staffed by people who could have asked, and sooner or later the record reaches the question of whether any of them did.

## THE THIRD PARTY

The [Office of Civil Surveys](#) is a letterbox, a name on the door, and a mandate nobody has ever summarised in fewer than four pages. You are a civic function and not a security service. That distinction is maintained carefully, in writing, by people who understand exactly what it is for.

What you hold is the aggregate. Not one client's data but the correlation across all of them. No single security stack can produce that view, and it is the only one worth having. When two organisations that acknowledge no relationship are in steady contact, the traffic says so whatever they say. You supplied the tooling for this. Note the order of events: the capability was wanted before it was offered.

You would like the feed to continue and nobody to mention it. If some of it does surface, you would like it credited to analysis of observed activity, true enough, and not to a source, equally true and less convenient.

Your options are to keep receiving, to let the thing surface and lose the source, or to send somebody round to suggest that a more measured account would suit everybody. You have done the third twice already. Both times the suggestion arrived before the finding it appeared designed to soften had been published. The MCLU has written that down.

Nothing was authorised in writing, because written authorisation leaves a record of responsibility. That absence makes it harder to prove you began this. It does not make it less true, and our assessment is that you bear the weight of it.

The temptation is to stay silent and remain a civic body receiving submissions from independent parties, while the record notes, accurately and uselessly, that no response was received.

## THE CLIENT

You are the Royal Bank, and the merchant guilds keep their books alongside yours. You did everything properly, which is the part worth sitting with.

You engaged the provider because you wanted better security, and then you behaved like an organisation that wanted better security: assessments run, configurations hardened, incident response practised until it was dull. Around you are the others who did the same. The Seamstresses' Guild. The Engravers'. The Home for [Bewildered Beasts](#), with its donor rolls and fifteen years of testimony from half the Disc.

Your exposure scales with how thoroughly you engaged. The vulnerability assessments you commissioned in good faith are a candid catalogue of your own weaknesses, produced by you, at your expense, now sitting with somebody you have never met. Your clearing volumes are observable whether or not you publish them. Your late-night correspondence with your legal advisors says a thing the contents of those letters never had to.

You want two things and only one of them is available. The security you paid for, which you did get. And an account of what else was happening while you got it, which nobody has offered.

You could act at once. You could first find out what was seen and across how long. You could tell your members and customers, or decide their exposure is yours to carry quietly on their behalf. You are entitled to decide that, and you will have to defend it. You will need to revise the threat model on the basis that your operating history and your known weak points are held by a party with no obligation to you.

The thing you will want to do, this afternoon, is force a visible change before you know what was taken. That shuts the stable door loudly, and tells whoever is watching which horse you valued.

## THE PROBERS

You are the [Scarlet Semaphore](#). Start with the part you did not know until this morning. The apparatus saw you. It logged the probing, decided it was reconnaissance and not attack, wrote down your methods, and passed all of that along with everything else it collects. You signed nothing, agreed to nothing, and had no relationship with the provider at all. You are in the data regardless.

You are the guild for people who prefer their mischief in code rather than cudgel, and Operation Red Lantern is yours: announce a false but plausible path, watch which guilds panic and which never notice at all. Everything reversible, says the internal notice.

You understand how the city misdelivers itself. Useful knowledge, and written down nowhere. You also assume you are watched, because a number of your former members now work for the Department of Silent Stability and you have never established how many of your current ones do.

What you want is to learn how trust moves through the control plane without breaking the city, and without

becoming a subject the Patrician has to make a speech about. The moment stability stops being an assumption and turns into a topic, he starts offering people choices.

So: carry on, knowing the ground is instrumented. Or redesign the operation around a watcher who logs and forwards and never intervenes. Or stop, and spend awhile wondering what stopping tells the party that has been reading you.

The instinct in the room will be to treat detection as failure and go dark. Consider the other reading. You have found a second watcher on the same wire, one that answers to no control room anybody can name, and that is worth more than an uninterrupted probe.

## **THE INVESTIGATOR**

You are the MCLU. You read the nineteen-page client agreement, and then the twenty-three-page enterprise version, because that is the service you provide and the reason you have no money.

You established the arrangement. Then you established something less comfortable. You are inside it. Your correspondence, your documents and your enquiries have gone through infrastructure connected to the provider's network. So has everything

your sources sent you. You did not know that when you began.

What you have is the record. Formal enquiries submitted and logged. The courteous reply with nothing in it, noted as a response, because it was one. Both intermediary approaches written down, since documenting them costs you less than it costs the other party. And a pamphlet, more use than it sounds.

What you want is modest on purpose. The clients told. The arrangement disclosed. The data accounted for. The third party named. And a rule that requires consent before this sort of tooling goes onto anybody's systems. The minimum, because the minimum can actually be got, and everything else is built on top of it.

You can publish on what you hold, or wait for evidence that survives a barrister. You can name the third party from your own assessment, or hold the name until you can stand behind it in a room. You can route around the provider, while saying in public that you are publishing this on a platform that may be read.

Waiting is the respectable choice and it has a cost. The arrangement continues while you wait. The one tool the apparatus cannot turn to its own use is your willingness to say, imperfectly and on the record, what you have found so far.