NORTH★STAR

RISING TIDE

Session 1

Conscience Doesn't Scale

INTRODUCTION

As technicians, we frequently face complex decisions unrelated to the underlying technology we support. Jiminy Cricket's "let your conscience be your guide" sounds nice, but the work isn't quite that simple.

Most of us never learned how to evaluate these judgment calls. Sure, we know to report exposed patient data or illegal content. But what about the gray areas? What happens when we see an employee stealing time, or hear about upcoming layoffs?

When we have a choice to make, there's more to it than experience and what ***feels*** correct. This guide reviews the tools we discussed to help with those evaluations, for when Jiminy Cricket's advice isn't enough.



Universities teach entire courses on ethical philosophy. The frameworks below are simplified for everyday use.

RULES, OUTCOMES, TRAITS

When facing an ambiguous decision in tech, start by asking yourself the three questions below.

In the field, these questions frequently conflict, such as situations where violating a "Rule" is the only way to produce a good "Outcome".

This is a lens. Be careful not to think of it like a checklist. Use it to uncover where the friction lies so you can make an intentional, defensible choice.

with Matt Topper and Mendy Green

Conscience Doesn't Scale

Rules (Deontology)

The Ask	Am I breaking a duty, a policy, or the law?
The Idea	Some actions are right or wrong regardless of how they turn out.
The Risk	Policies often lack nuance and can't anticipate every situation. When a situation needs an exception, the other questions help you decide.

Outcomes (Consequentialism)

The Ask	Who is helped or harmed by this? What's the impact?
The Idea	An action is judged by its results, whether or not a rule covers it.
The Risk	It's often impossible to know the result ahead of time, and you're taking a chance.

Traits (Virtue Ethics)

The Ask	What would someone I respect do here? Am I OK with my name on this?
The Idea	Ethics is ultimately about character. In short: "Would you make the same decision if nobody knew?"
The Risk	It relies on personal intuition and can lack concrete guidance when two "good" traits (like loyalty to your team vs. honesty with the client) conflict.

R/O/T Example

Scenario: Mouse Mover

You find auto_mouse_mover.exe on a remote employee's laptop, which keeps their status "Green" all day. This client's leadership is openly against remote work and has been looking for a reason to return to office.

Rules This almost certainly breaks the acceptable use policy. Tell the client's primary contact.

Outcomes Notifying the contact may cause the client to end remote work for everyone, or even fire the employee.

Traits Picture a tech you respect and ask what they'd do. They'd be honest with the client and fair to the employee, and here those conflict.

Each lens points to a different answer, based on its own loyalty. The decision is still yours, and now it's an informed one. It's the same thing we ask of clients: they can decline the MDR service, as long as they understand the risk they're accepting.

MORAL DISENGAGEMENT

Psychologist Albert Bandura spent decades studying how decent people end up doing things they know are wrong. He called it **moral disengagement**. Your values stay where they are, and you'd still say that ignoring a problem is wrong. You just decide, quietly, that this one doesn't count, or that it isn't yours to deal with. Since nothing about what you believe has changed, there's no guilt to warn you.

It usually happens without much thought, and it gets easier with practice. An excuse that took some convincing the first time is routine by the fifth. Bandura identified eight of these mechanisms, and most of them show up regularly in IT work. Each one is easier to catch once you know what it sounds like.

Conscience Doesn't Scale

DISPLACEMENT OF RESPONSIBILITY (OBSCURING YOUR RESPONSIBILITY)

The Temptation A client asks you to disable their firewall so a line-of-business app can pull an update. You know nobody will remember to ask for it to be turned back on. You disable it and close the ticket.

The Voice "They asked for it. It's in the ticket."

DIFFUSION OF RESPONSIBILITY (OBSCURING YOUR RESPONSIBILITY)

The Temptation While closing a printer ticket, you notice a server that hasn't been patched in months. It isn't your account, and you have eight tickets waiting.

The Voice "There's a whole team on this client. Someone must be dealing with it already."

EUPHEMISTIC LABELING (REFRAMING THE ACT)

The Temptation A project ran well over its time budget because the client kept adding scope. Writing up a change order means an awkward conversation about more money.

The Voice "I'll absorb the hours. It's an investment in the relationship."

ADVANTAGEOUS COMPARISON (REFRAMING THE ACT)

The Temptation Restoring a file took 15 minutes, but you bill 30 to keep your utilization numbers up.

The Voice "Dave logs a full hour for this."

MORAL JUSTIFICATION (REFRAMING THE ACT)

The Temptation You set up a new PC for a user. Their printers and a couple of apps they use every day aren't in the standard deployment, so you skip them.

The Voice "They shouldn't be using anything that isn't deployed through Intune anyway."

MINIMIZING CONSEQUENCES (DOWNPLAYING THE CONSEQUENCES)

The Temptation A client who's had a rough month emails you directly instead of opening a ticket. A few days later, they're annoyed they haven't heard back.

The Voice "If it were important, they'd have sent it to support."

ATTRIBUTION OF BLAME (DEVALUING THE PERSON AFFECTED)

The Temptation You're replacing a user's laptop. Their personal photos don't make it over.

The Voice "Not my fault. They stored them on the root of C:."

When you catch yourself using one of these phrases, it's a sign to take a second look. The risk with moral disengagement is that the arguments ***are*** valid through the right lens. Make sure that you're making an intentional choice, instead of using these to sidestep the core decision.

LEGAL REQUIREMENTS

Sometimes the law decides for you. Therapists face a version of this. In ***Tarasoff v. Regents of the University of California*** (1976), the California Supreme Court held that a therapist's duty to protect someone from a credible threat of violence outweighs patient confidentiality.

Our access to client systems puts us in a similar position. Keeping what we see private is the default. The law requires us to break that default in a few cases, fewer than most techs expect.

Regulated Data: If you find exposed PHI or CUI, or customer records that may have been breached, report it through your company's incident process. Many regulatory bodies require reporting data leaks.

Note that writing "you need to report breaches to us" on a spreadsheet of certification requirements or in a company policy manual doesn't create a legal duty. For the employee, the consequence is losing their job, not legal action. Similarly, the consequence from a certification body is to revoke the certification. Legal obligations come from laws or from contracts. Neither spreadsheets nor policies are those.



If you ever see child sexual abuse material on a system, stop. Don't copy files or image the drive, since copying it can be a crime in itself. Report it to law enforcement or NCMEC's CyberTipline, and let your company's leadership know. Several states require computer technicians to report it, and the rules vary, so check yours. Either way, treat reporting as mandatory.

Everything Else: Outside of those specific instances, the law asks surprisingly little of us as techs. This is where ethics come in. Finding evidence that an employee is stealing from the company or leaking its data generally doesn't create a legal duty to report, as long as you don't destroy evidence or lie about what you saw. The same goes for personal lives. The law doesn't require notifying anyone if you see evidence of an affair, for example. In fact, even seeing evidence that someone is in danger usually doesn't ***legally*** require taking action, though the obvious step is to notify authorities.