the randomised response method

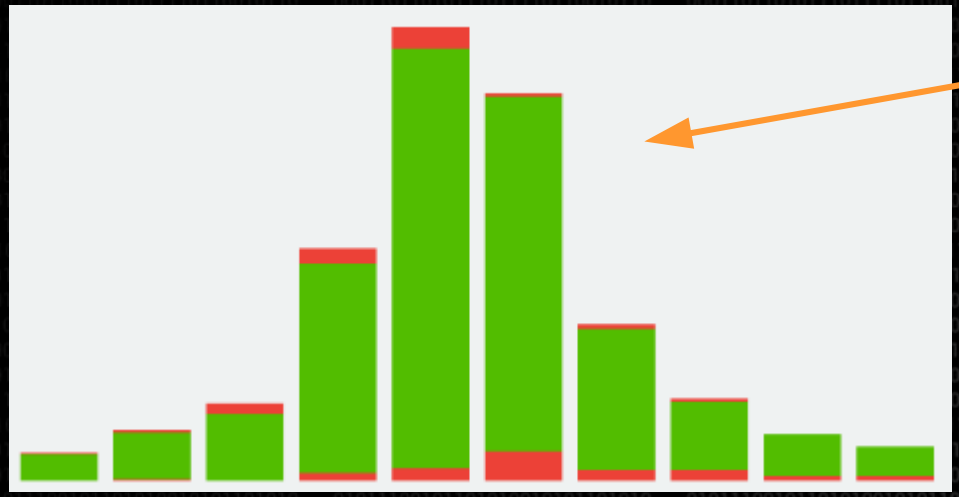
or,

how to collect data about your users without doing things that should make them hate you

@sil

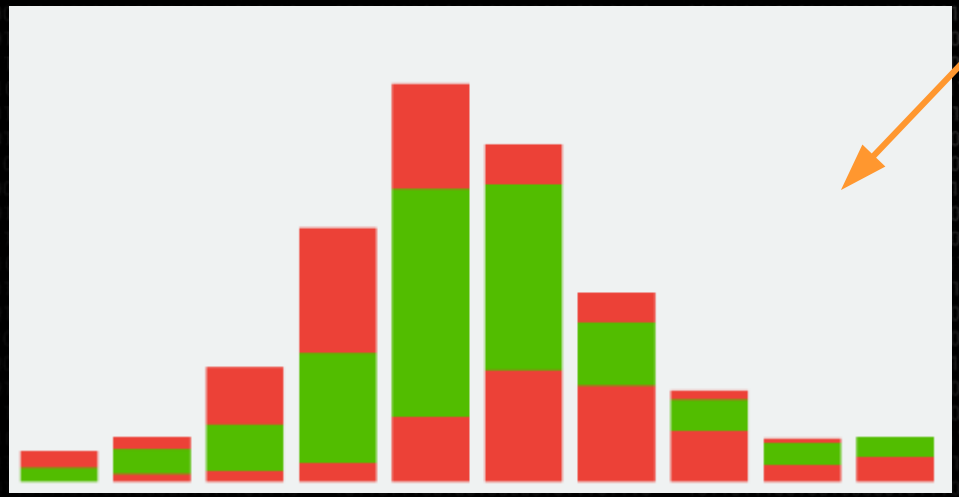
@sil

kryogenix.org

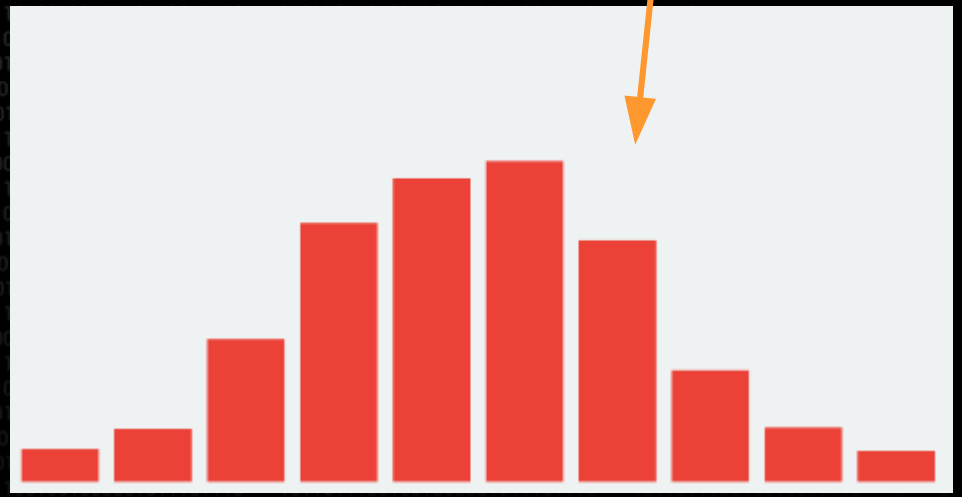


mostly truth

half
and
half



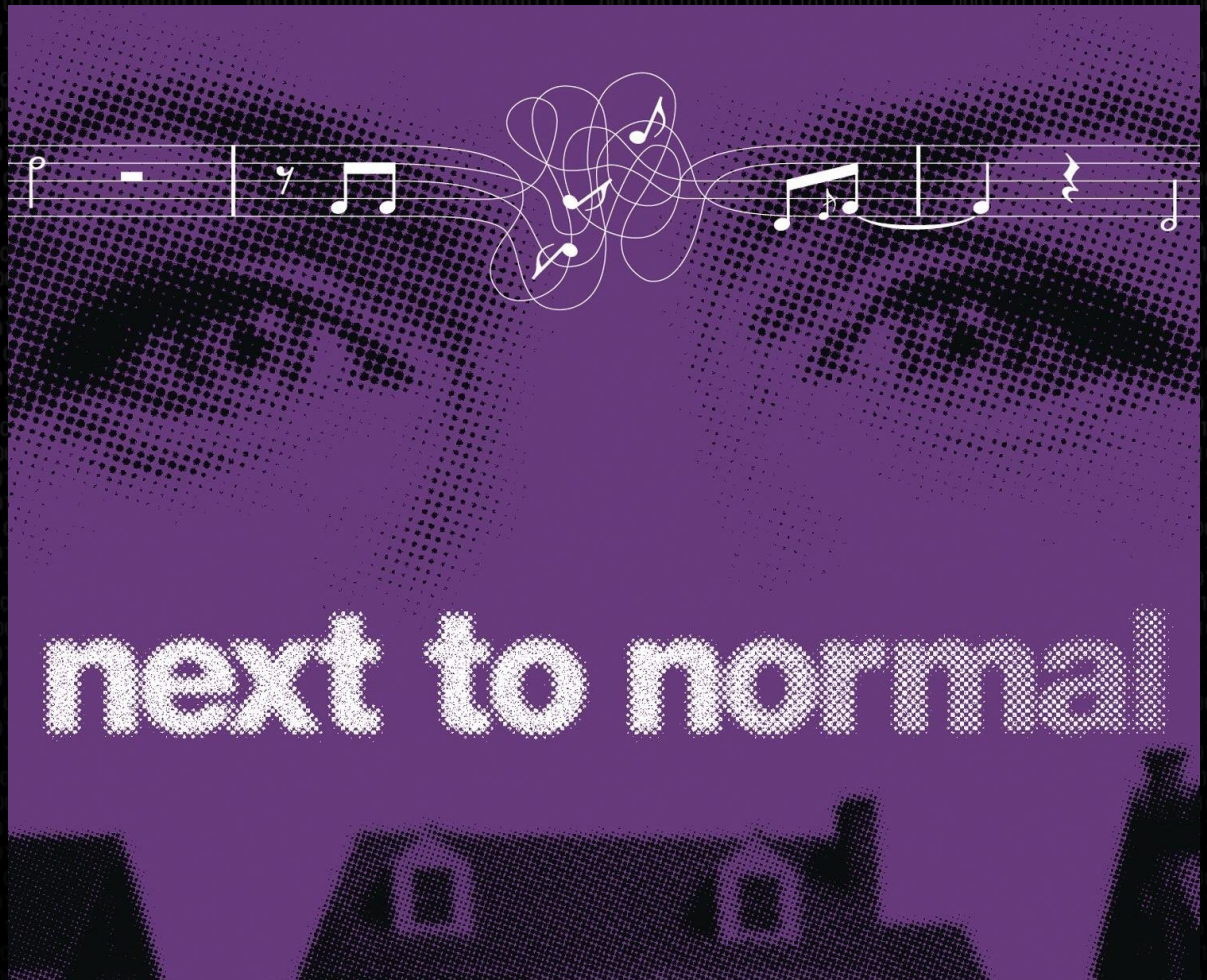
lies, all lies



```
user_answer = ask_user_question()
if (chance < 20%) {
    change_user_answer()
}
```

@sil

kryogenix.org

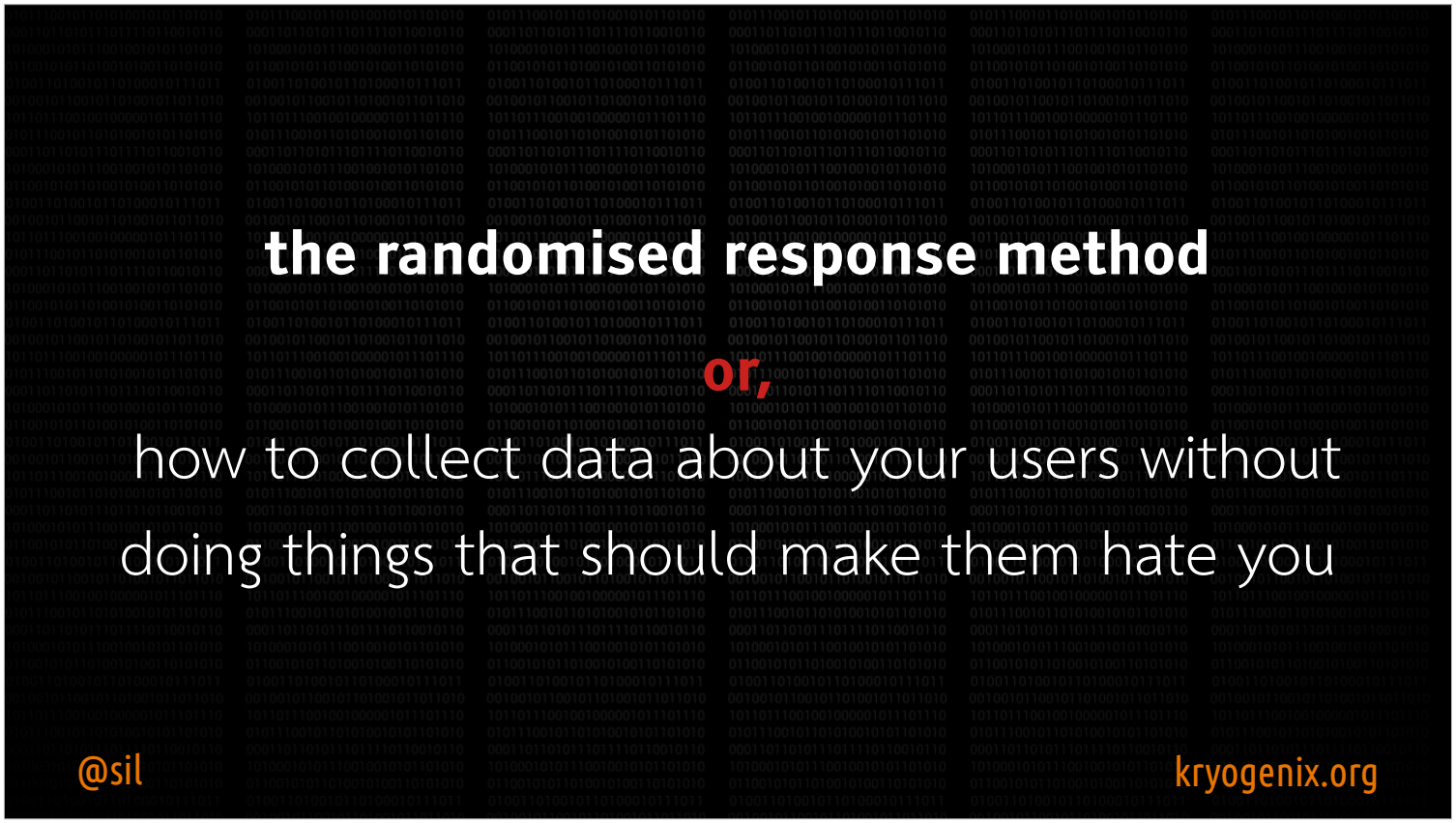


@sil

kryogenix.org

@sil

kryogenix.org



There are lots of people in this audience, me among them, who would say: hey companies, stop collecting data about everyone and using it to do evil things!

But they *mostly* aren't being deliberately evil.

We want people to be data driven, right?

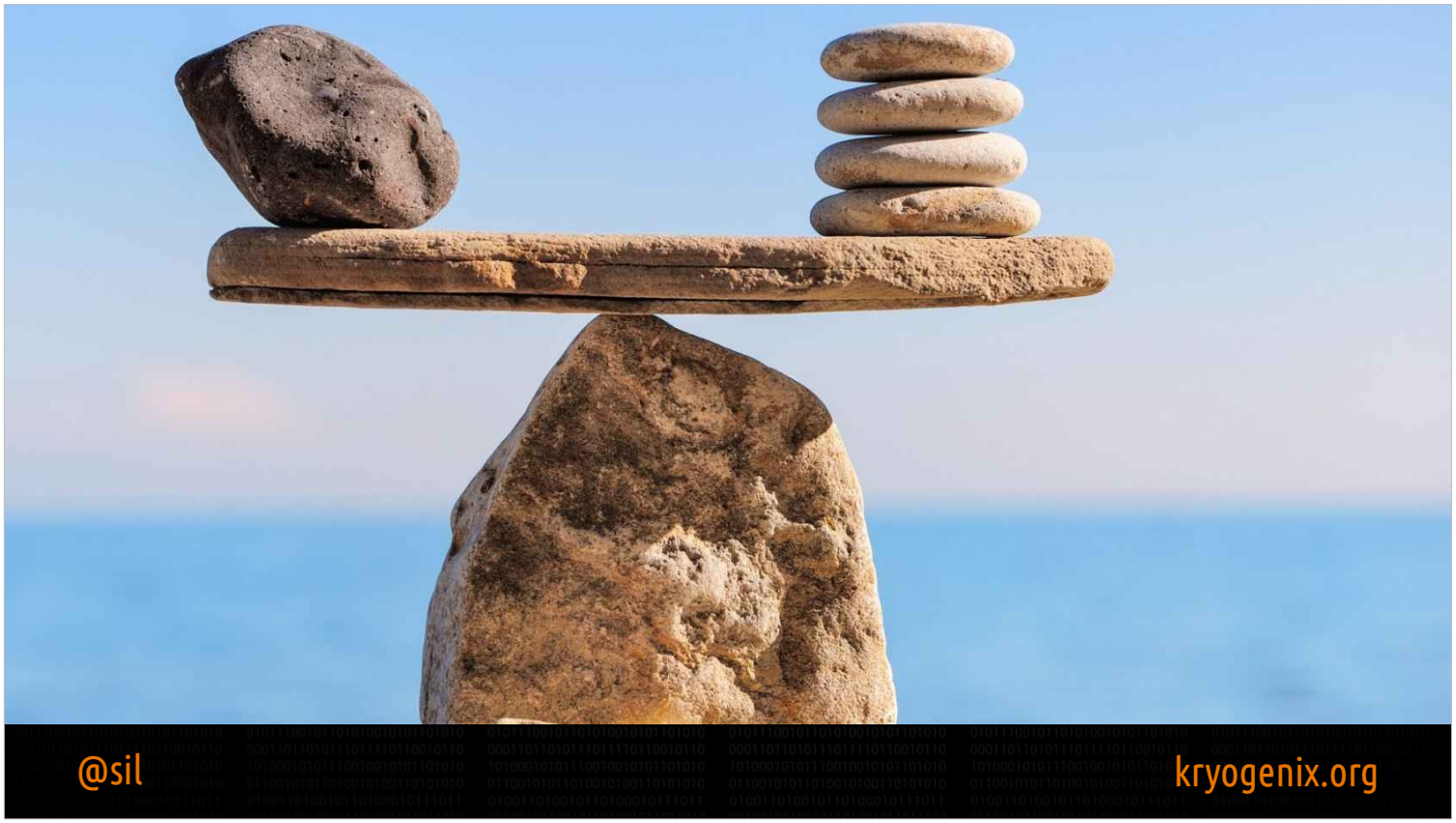
We just want that data to not compromise us.

This problem was faced by people in the 1960s too, doing surveys. Let's say you are John F. Kennedy and you're thinking about whether to legalise marijuana. So one thing you want to know is: how many people are currently using it even though it's illegal? So you do a survey. You ask people: have you used marijuana? And what happens?

Well obviously everyone lies. I mean, you're the Man; if your interviewees confess then you kick down the door and put them in Shawshank Prison or something. So what you need is a way to ask the question and get answers and rely on those answers but without requiring people to criminally incriminate themselves to answer.

So if you're a clever researcher in the 1960s then you invent the *randomised response method*. This is how it works. You ask people: have you smoked dope? And then you ask them to secretly flip a coin. If the coin comes up heads, then they tell the truth, and if it comes up tails then they lie. So if you *have* smoked, and your coin comes up heads, then you say "yes I have". If you have smoked and your coin comes up tails then you lie and say "no I haven't", even though you have.

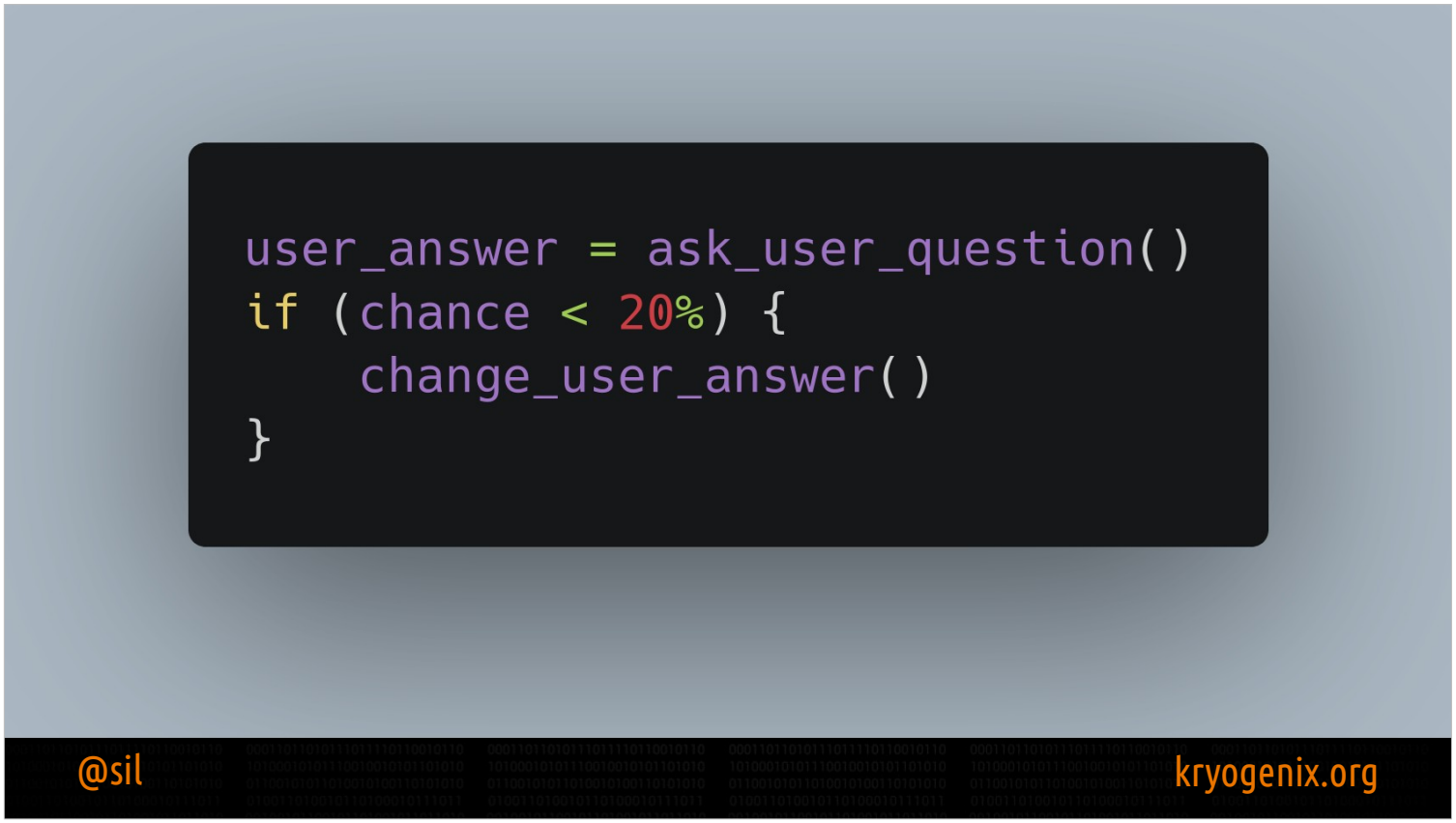
The beauty of this is that any one person's answer is not incriminating. If the cops boot down the door and say; you confessed! Then **you** say: nah, my coin came up tails, so I was lying.



And the good thing about this is that the survey is still reliable, because all the errors cancel out! If you do this survey, and 20% of the population have smoked weed, then in your survey results you'll see that roughly 20% of the population have smoked weed *even though any one given person's answers are not reliable*. So you get the correct answers but people's data is safe!

And this works on more than just binary yes/no choices. You can ask people any multiple-choice question, and give them any percentage chance of lying – 50% with a coin flip, or 10%, or whatever – and this still gives you results you can interpret and understand. Let's take a look at some examples in more detail.

We want to collect data about people's ages. So we ask them which age range they're in – 18-24, 24-35, etc. But we also tell the, with a certain percentage chance, lie about your answer; so 90% of people tell the truth, 5% of people lie and say they're younger than they are, 5% lie and say they're older. On these graphs, green is people who told the truth, red is people who lied. And you can see that the shape of the graph is fairly constant! If we make 50% of people lie, like the coin example, it still works. Even if you make **every single person lie**, so your survey does not have one single correct answer, the shape of the graph is still *roughly* correct. So what this means is that you can "tune" how much you want data accuracy versus how much you protect user privacy.



The important thing about this is that this is not some weird statistical technique that you need to be a mad data scientist to use. You can do this now. Literally any time your UI asks users a question about themselves, assign a percentage chance of lying, and have the UI change their answer.

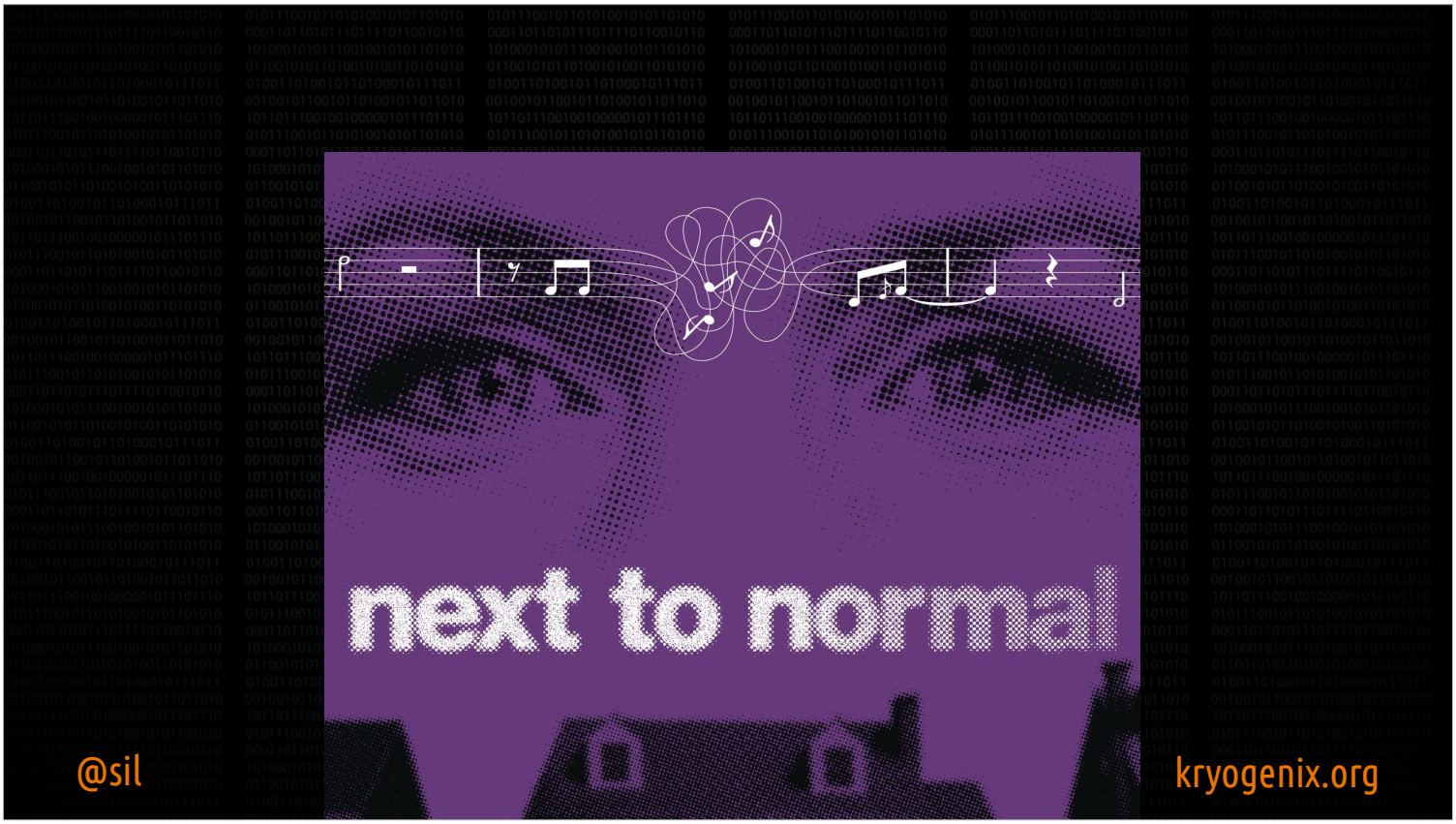
Then store that in your DB.

What it’s important to get across here is that there is a Middle Way. We’ve been kinda presented with a binary choice: bad evil companies collect data about you and use it for nefarious purposes, and your choice is either to suck it up or to opt out entirely. And sure, opting out entirely is one approach; how many people in here use Facebook? Not many, I guess.

But you shouldn’t *have* to opt out. A person who’s now 20, like my daughter, has *never known the experience of being lost*. I can think of a song I haven’t thought of for years and then ask for it, literally by saying the words aloud, and it plays. This is like being Merlin! It’s cool! We shouldn’t have to choose between superpowers plus no privacy, or privacy plus no superpowers.

So this is something you can do, those of you who are developers, or business analysts. Go back to your companies and your projects and say: let's let people lie. Let's get the data we need to make smart competent decisions *without* demanding that users give up their inside leg measurement and everywhere they've ever been to get it.

This is a *selling point* for your company. You can trade on this, and it doesn't affect anything else you're doing. You don't have to give anything up to get this; there's no tradeoff. Your data quality stays roughly the same, and your users' privacy is more protected; users who care like that, and users who don't care aren't affected, so this action is completely positive.



This is really about normalisation. The stuff that people in this room build, and help to build, controls a surprising amount of the world. But it's often hard to see how you can make a change that has a long-term effect; you're doing good decent work and then some mysterious Other company collects all this info about you and uses it to make worrying and creepy decisions.

Well, this is something you can do. And what that does is that it teaches real people, the people who *use* the stuff you build, that it's *OK to ask for this*. That it is reasonable to expect a middle way. That there is some way they can vote with their feet by choosing products that protect them, but without voting with their feet by avoiding the whole internet and not talking to their friends.

So, that's me; if you want to know more about this I'll be in the pub, and I'm giving a talk tomorrow in Ballroom C, and I'm @sil on twitter, so I'm happy to come talk to you or your company or whatever. Thank you very much.