Control as Liability

2019 May 09 See all posts

The regulatory and legal environment around internet-based services and applications has changed considerably over the last decade. When large-scale social networking platforms first became popular in the 2000s, the general attitude toward mass data collection was essentially "why not?". This was the age of Mark Zuckerberg saying the age of privacy is over and Eric Schmidt arguing, "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place." And it made personal sense for them to argue this: every bit of data you can get about others was a potential machine learning advantage for you, every single restriction a weakness, and if something happened to that data, the costs were relatively minor. Ten years later, things are very different.

It is especially worth zooming in on a few particular trends.

- **Privacy**. Over the last ten years, a number of privacy laws have been passed, most aggressively in Europe but also elsewhere, but the most recent is the GDPR. The GDPR has many parts, but among the most prominent are: (i) requirements for explicit consent, (ii) requirement to have a legal basis to process data, (iii) users' right to download all their data, (iv) users' right to require you to delete all their data. Other jurisdictions are exploring similar rules.
- **Data localization rules**. India, Russia and many other jurisdictions increasingly have or are exploring rules that require data on users within the country to be stored inside the country. And even when explicit laws do not exist, there's a growing shift toward concern (eg. 1 2) around data being moved to countries that are perceived to not sufficiently protect it.
- **Sharing economy regulation**. Sharing economy companies such as Uber are having a hard time arguing to courts that, given the extent to which their applications control and direct drivers' activity, they should not be legally classified as employers.
- **Cryptocurrency regulation**. A recent FINCEN guidance attempts to clarify what categories of cryptocurrency-related activity are and are not subject to regulatory licensing requirements in the United States. Running a hosted wallet? Regulated. Running a wallet where the user controls their funds? Not regulated. Running an anonymizing mixing service? If you're *running* it, regulated. If you're just writing code... *not regulated*.

As Emin Gun Sirer points out, the FINCEN cryptocurrency guidance is not at all haphazard; rather, it's trying to separate out categories of applications where the developer is actively controlling funds, from applications where the developer has no control. The guidance carefully separates out how *multisignature wallets*, where keys are held both by the operator and the user, are sometimes regulated and sometimes not:

> If the multiple-signature wallet provider restricts its role to creating un-hosted wallets that require adding a second authorization key to the wallet owner's private key in order to validate and complete transactions, the provider is not a money transmitter because it does not accept and transmit value. On the other hand, if ... the value is represented as an entry in the accounts of the provider, the owner does not interact with the payment system directly, or the provider maintains total independent control of the value, the provider will also qualify as a money transmitter.

Although these events are taking place across a variety of contexts and industries, I would argue that there is a common trend at play. And the trend is this: **control over users' data and digital possessions and activity is rapidly moving from an asset to a liability**. Before, every bit of control you have was good: it gives you more flexibility to earn revenue, if not now then in the future. Now, every bit of control you have is a liability: you might be regulated because of it. If you exhibit control over your users' cryptocurrency, you are a money transmitter. If you have "sole discretion over fares, and can charge drivers a cancellation fee if they choose not to take a ride, prohibit drivers from picking up passengers not using the app and suspend or deactivate drivers' accounts", you are an employer. If you control your users' data, you're required to make sure you can argue just cause, have a compliance officer, and give your users access to download or delete the data.

If you are an application builder, and you are both lazy and fear legal trouble, there is one easy way to make sure that you violate none of the above new rules: *don't build applications that centralize control*. If you build a wallet where the user holds their private keys, you really are still "just a

software provider". If you build a "decentralized Uber" that really is just a slick UI combining a payment system, a reputation system and a search engine, and don't control the components yourself, you really won't get hit by many of the same legal issues. If you build a website that just... doesn't collect data (Static web pages? But that's impossible!) you don't have to even think about the GDPR.

This kind of approach is of course not realistic for everyone. There will continue to be many cases where going without the conveniences of centralized control simply sacrifices too much for both developers and users, and there are also cases where the business model considerations mandate a more centralized approach (eg. it's easier to prevent non-paying users from using software if the software stays on your servers) win out. But we're definitely very far from having explored the full range of possibilities that more decentralized approaches offer.

Generally, unintended consequences of laws, discouraging entire categories of activity when one wanted to only surgically forbid a few specific things, are considered to be a bad thing. Here though, I would argue that the forced shift in developers' mindsets, from "I want to control more things just in case" to "I want to control fewer things just in case", also has many positive consequences. Voluntarily giving up control, and voluntarily taking steps to deprive oneself of the ability to do mischief, does not come naturally to many people, and while ideologically-driven decentralization-maximizing projects exist today, it's not at all obvious at first glance that such services will continue to dominate as the industry mainstreams. What this trend in regulation does, however, is that it gives a big nudge in favor of those applications that are willing to take the centralization-minimizing, user-sovereignty-maximizing "can't be evil" route.

Hence, even though these regulatory changes are arguably not pro-freedom, at least if one is concerned with the freedom of application developers, and the transformation of the internet into a subject of political focus is bound to have many negative knock-on effects, the particular trend of control becoming a liability is in a strange way *even more pro-cypherpunk* (even if not intentionally!) than policies of maximizing total freedom for application developers would have been. Though the present-day regulatory landscape is very far from an optimal one from the point of view of almost anyone's preferences, it has unintentionally dealt the movement for minimizing unneeded centralization and maximizing users' control of their own assets, private keys and data a surprisingly strong hand to execute on its vision. And it would be highly beneficial to the movement to take advantage of it.