While we all might be aware of cybersecurity, there is considerable confusion as to what it actually is, and who it serves to protect. Much of the media conversation around cybersecurity is couched in the language of protecting state interests against “bad players” in the digital ecosystem, such as hackers. The standard media depiction of hackers are as study individuals lurking in a maze of binary, leveraging their expertise to target the innocent and the vulnerable.

The messaging of the state is that it can protect you only if you expose all your data to its paternalistic patronage, positioning itself as a safe haven and trusted repository with the citizen’s interests at heart. Ideally, however, cybersecurity should be inseparable from individual privacy, and be exercised as a human right. This sets up an opposition between privacy and (state) security; the latter a state mandated obit which undermines rather than refines individual privacy.

The ideal way to understand the relationship between the two is that privacy can lead to better security. In our illustrations, we have tried to decide and respond to the assumptions that underpin commissioning of illustrations of cybersecurity for the mainstream media. The messaging of the state is that it can protect you only if you expose all your data to its paternalistic patronage, positioning itself as a safe haven and trusted repository with the citizen’s interests at heart. Ideally, however, cybersecurity should be inseparable from individual privacy, and be exercised as a human right. This sets up an opposition between privacy and (state) security; the latter a state mandated obit which undermines rather than refines individual privacy.

The complexity of everyday technology use, social media, platform governance, consent and privacy, is a part of some of the narrative and can be seen, in this case, to manifest, by using old tropes—such as icons of keys, locks, doors, silhouetted characters in hoodies, footprints, screens, lines, icons of code-leaking, magnifying glasses, finger prints, van cameras, hooks, fishes and the old badge with chains—taking them out of context, subverting them and sometimes the amplification of older meanings at newer scales. There is an effort to show the intended manifestations of technology in the form of physical gestures, ephemeral experiences, triggered and realized services and the very real physical infrastructures alongside the very actual humans and their data. The research underpinning these illustrations have also been about play, how devising a platform to say or show things that might otherwise be difficult to transition through texts, or to see both in detail and as a whole or might seem ludicris. Some of these manifest when the unintended networking of many of these services allows for incredibly unulated flow and access of data and more so the metadata trails from these intended technologies.

What follows from the first panel up till the last is an expression of, what may be understood as behaviors around and through digital technologies, that allow for networked-computer computation, at various scales.

Panel 1

This is a depiction of individual to individual interactions, where our devices allow for mediated experiences, from a range of new enablers to financial transactions and everything in between. Some of the sketches are observations of people largely in common across networked spaces like coffee, which become second spaces for conversations and sometimes for filing taxes. Contrary to popular depictions of the man in the hoodie trying to take advantage of vulnerable linked devices, there were several simpler opportunities of violating somebody’s notion of private access to their data in public spaces and personal details like name (that is generally made audible in places like Starbucks), system id (that is accessible if a device is left unattended), or details ever heard during a personal conversation in a public space, become data that may be acquired by people either directly looking for it, or found through indexed or hash-tagged images on networked and multi- platform behaviors.

Panel 2

The second panel is the first instance of trying to look at complexity from the perspective of larger instances, that one must create data and services around instead for individuals. On the top side, there are ethical hackers previously labelled (by projecting a caricatured notion of the Wild West) as White hat hackers, who typically look at possible loopholes or aberrations in privacy, access protocols that might render a service vulnerable for either institutions or individuals, or both. Ethical hacking for instance may involve bug bounty hunting, that may result preventing future breaches in large volumes of user and institutional data. These activities may also result in identifying malicious intent also in the part of institutions as plying upon its users by manipulating their behavior.

Panel 3

The third panel was an exploration of how notions of user generated content (UGC) and behaviors because of it could be leveraged by larger institutions or the interaction of institutions with, for or against individuals. Some of the explorations as a result, are around click-farms and behaviors of collusion. There is a small satirical attempt here to contextualize the notion of Hobbes’s Leviathan with a slightly more familiar (Indian) context of Dineshan. This diegetic, also looks at the emergence of Directed behaviors that lead to state sponsored surveillance, internet shutdowns and military coups, that is framed in ways that show the state and its citizens as an invasive agent, in some online spaces, or as justified in its actions in dominant news narratives.

Panel 4

The fourth panel started out as a composition that shows interactions between and across different institutions and various states. It moves forward the concept of a corpus of consent, manufactured or elected, through computer mediated spaces. Using the framework of Dineshan, this panel meditated on an interaction of many dimensions among themselves, against other dimensions and the impact it may have on concepts of privacy, security and governance in a networked age. Once the composition was created, it also became a point of reflection of local or personal behaviors on mediated platforms. As depicted is one of the themes paves about existential dread that emanates from interacting with others on computer mediated platforms, the user @sadgurlmemez, describes attributes of being directed at a more local and personal level, where one aspect of it is cultural in nature, where one performs many different aspects of themselves, in public computer mediated spaces, thereby creating the data trail that has been seen from panel one.