Missing rigour and due diligence

Subhashis Banerjee*
Computer Science and Engineering
IIT Delhi

June 18, 2023

The recent media reports about CoWin data leak are no doubt disconcerting, but what is even more disconcerting is the government response to these reports. It is hardly reassuring for us to know through a ministerial declaration that though some data may have leaked due to earlier breaches or poorly modelled use cases, there really is nothing to worry because the backend database is probably still secure. The question is – from what?

Data related privacy and security concerns are usually countered with two kinds of reactions. The first are fatalistic, and they dismiss the worries saying that our phone or Aadhaar numbers may already be out there with hundreds of entities anyway. These reactions are frivolous and are not to be taken seriously. Various data protection discourses and the supreme court judgement on privacy debunk these adequately. The second are from the keepers of these systems, and they often claim security by forceful proclamations. They argue that the security and privacy safeguards deployed are foolproof because they use "state-of-the-art best practices". These claims often fail to precisely articulate what are the exact security and privacy problems that these best practices address and investigate, and end up by affirming – ad nauseam – that "the backend databases are safe and we have taken care of privacy". Unfortunately, that is neither here nor there.

Security and privacy discourse requires a standard grammar to ensure that the stakeholders do not talk past each other. It is customary in contemporary computer science to start security specifications with a well-articulated threat model which precisely captures the security risks and the capabilities of a hypothetical adversary. For large public service applications involving critical personal data, it is standard to assume that the adversary can corrupt all insiders - including system administrators of compute, storage, cloud, and authorisation systems – all custody chains and all hardware and software. Then, the system designers are required to either convincingly argue security – in some well-established and standard (usually cryptographic) framework – against such a threat model, or clearly specify the unavoidable trust assumptions on various authorities. Trusting the integrity of software or hardware is usually avoided because such verifiable correctness is often intractable to establish. Solutions are typically acceptable only if the trust can be distributed among multiple authorities and it can be demonstrated that a system is provably safe unless a threshold number of the authorities collude. These standards are undoubtedly hard to achieve, which is one of the main reasons because of which digitalisation attempts are conservative in most countries. Unfortunately, none of the large public service digitalisation undertakings in India probably measure up to these standards. They do not even have publicly articulated threat models without which the security claims are at best imprecise and at worst vacuous.

Privacy requires even more due diligence. Leakage of sensitive personal information like DOB, phone, Aadhaar or passport numbers not only makes one vulnerable to direct harms like frauds,

*Opinions expressed are personal

identity thefts or illegal surveillance, but also to hard-to-detect indirect harms resulting out of unknown entities using personal information in unknown ways. For example, such data may be used illegally for profiling voters and influencing them for elections, or for profiling people for predatory marketing or advertising. This is particularly problematic because individuals are often less careful about these indirect harms, but the collective harm to the society is considerable. Indeed, the privacy judgement of the supreme court has identified loss of informational self-determination as a perilous privacy harm which the government is duty-bound to protect us from in all its digitalisation endeavours.

Preventing such function creeps requires exacting standards of purpose limitation, for which security – particularly against insider attacks – is an obvious necessary condition. However, it is by no means sufficient. Also required are legal standards of purpose limitation and access control regulations to prevent building parallel copies of sensitive databases. Any digitalisation necessarily entails some privacy risks at the interface of the digital and the human. The interface is a crucial component of the digitalisation use cases, which define how various users – including administrators and operators – interact with the digital systems. There always are some inevitable information leaks at these interfaces which need to be precisely modelled. This requires not only modelling the communication protocols and edge devices for data recording and dissemination, like point-of-service systems or phones, but also the privacy impacts of the information that is revealed to operators and entities. It is incumbent upon the system designers to precisely model this minimum unavoidable risk in an ideal functionality, and verifiably demonstrate that system implementation does not introduce any additional risks. Precise modelling of the minimal unavoidable risk is also necessary to evaluate the proportionality of the digitalisation application by weighing the risks with the benefits, which is the basic test prescribed by the supreme court to judge constitutionality of public service applications.

Failure to do the required due diligence of privacy risk assessment of use cases invariably results in function creeps and violations of purpose limitation, as is evident from the imprecise definition (in the Aadhaar Act) and the indiscriminate use of the "Aadhaar card" in all sorts of services. Some of these are backed by laws and some are not. It is not surprising that there are inevitable privacy breaches, and every now and then one hears about some or the other data leaks and misuses of Aadhaar.

The other harms that often arise due to inadequate modelling of use cases are in digitalisation of welfare delivery such as sale of PDS ration or MNREGA payments. Failure to precisely understand the constraints on equipment, users and personnel, their digital literacy levels and empowerment, and the relationship of the primary function of the welfare service with the digitalisation may result in exclusions and denial of services, hardships, and increased transactional costs for the beneficiaries that may ultimately hurt the very objectives of the welfare services. Indeed, there are reports abound of such harms from all around the country.

The digitalisation journey in India has been breathtaking in its scale and scope, and, given our challenges, we perhaps need digitalisation of public services more than most others. However, the digitalisation can certainly do with some more computer science rigour.