

Authorisation and access control architecture as a framework for data and privacy protection

Subhashis Banerjee

Computer Science and Engineering
IIT Delhi

30 January, 2018; updated on April 17, 2018

Abstract

Privacy protection in digital databases does not demand that data should not be collected, stored or used, but that there should be guarantees that the data can only be used for pre-approved and legitimate purposes. We argue that a data protection law based on traditional understanding of privacy protection and detection of privacy infringements is unlikely to be successful, and that what is required is a law based on an understanding of the architectural requirements of authorisation, audit and access control in real-time. Despite the protection principles being sound, privacy protection in digital databases has been less than effective, anywhere, mainly because of weak enforcement methods.

1 Introduction

The debate engendered by the identity project has suddenly propelled us from being a predominantly pre-privacy society to one in which privacy protection in digital databases has emerged as a major national concern. The welcome and scholarly Supreme Court judgment on the right to privacy [[The Puttaswamy judgment, 2017](#), [Bhatia, 2017b](#)] has made it abundantly clear that privacy protection is imperative, and any fatalistic post-privacy world view [[Spivack, 2013](#)] is untenable. Informational self-determination and the autonomy of an individual in controlling usage of personal data have emerged as central themes across the privacy judgment. See [[Bhatia, 2017a](#)] for a summary.

Recording transactions with a digital identity projects an individual into a data space, and any subsequent loss of privacy can happen only through the data pathway. Hence data protection is central to privacy protection insofar as digital databases are concerned. Two main uses of digitisation of transactions are accurate record keeping for audit and post facto investigation, and data analytics to discover useful patterns in the data. The latter can be particularly useful for econometric analysis, epidemiological studies and latent topic discovery. It can hence facilitate improved design of social policy strategies and early detection and warning systems for anomalies [[Agrawal et al., 2017](#)]. However, both record keeping and analytics can lead to potential loss of privacy. Long term storage of digital records, indexed by an identity, may result in unauthorised accesses which may violate personal data autonomy. Analytics often require joining of data from different domains to be able to mine useful knowledge. Such breaking of silos, in turn, can also be used to profile individuals beyond legal sanctions and can thus violate the principle of informational self-determination. Hence, effective use of digital databases and privacy protection have some apparently contradictory requirements.

In this note we investigate the possible ways in which such contradictions may be resolved. We also analyse the recommendations of the Srikrishna committee on a data protection framework [Srikrishna et al., 2017]. We argue that any solution that is solely based on detection of privacy violation and subsequent remedial action is unlikely to be satisfactory, and what is required in addition is an online architectural solution that prevents privacy invasions in the first place. As pointed out in [Raghavan, 2018], *ex-ante* rather than *ex-post* should be the preferred approach.

The welcome emphasis on data privacy provides us with a unique opportunity to take a fresh look at protocol design for effective digital services in India. On the one hand our systems should offer stricter privacy protection than what is prevalent in the US, where not only are identity theft rates unacceptably high [The London School of Economics and Political Science, 2005], but also where some of the world's largest corporate panopticons like Google and Facebook have grown more or less unchecked. On the other hand India should ideally have a more innovation friendly setup than what the European GDPR [The European Parliament and the Council of European Union, 2016] can offer, which perhaps is unduly restrictive but is unlikely to be commensurately effective. Moreover, our designs need to be specially sensitive to our large under-privileged population which may not have the necessary cultural capital to deal with overly complex digital setups.

2 Privacy risks in digital databases

The first step to privacy protection is to understand the ways by which privacy may be compromised in digital databases.

The most common fear of digitisation, especially when enforced by governments, is that of mass surveillance. All digitisation require unique digital identities, and the use of a universal identity in a multitude of databases can possibly create an infrastructure for totalitarian observation of citizen's activities across different domains. It may be naive to repose faith in benevolence of governments, anywhere, and the mere presence of an unrestricted surveillance infrastructure, which digital databases linked by unique identities can easily lead to, can potentially disturb the balance of power between the citizens and the state, stifle dissent and be a threat to civil liberty and democracy [Drèze, 2016]. Several commentators have used cliched metaphors like *Orwellian big brother* or *panopticon* to describe the situation.

A far more common and subtle manner of erosion of privacy is by the way of losing control of informational self-determination both to the state and to other seemingly mysterious, uncaring and opaque bureaucracies. Often there is no direct or obvious invasion of privacy, but because of the ease of replication, aggregation and selective combination of whole or parts of personal digital data, one may sometimes become unsure about what information about her is being used by the state and other bureaucracies and for what purposes. [Solove, 2004] argues that *Kafkaesque* is a more appropriate metaphor for describing this situation. Not only can personal information leach out and be used in unpredictable ways by unpredictable entities, but one can also be mis-profiled, wrongly assessed or even influenced [Confessore, 2018] using out of context data, without being able to control such decisions or sometimes even being aware of them.

Yet other typical pitfalls of bureaucratic digitisations are poorly thought out use cases, incomplete case analyses and incompetent programming. As common fallouts one may suddenly find herself being deregistered from services due to no fault of her's, or having to unnecessarily run around to get things corrected when she was not the one responsible for the mistakes in the first place. Being denied participation in school painting or dance competitions because of want of a national digital identity, or being denied hospital treatment, pension or welfare because perhaps a name is misspelt or because fingerprints do not match will be cases in point. Such callous omissions can not only be threats to right to privacy, but, in extreme cases, even

to rights to liberty and life [Banerjee, 2017].

Finally, threats to privacy and liberty also arise from big-data analytics or machine learning algorithms, which are important reasons for collecting and recording high frequency, real-time and non-aggregated transactional data in the first place. [O’Neil, 2016] forcefully argues that big-data analytics, by the very fact that they are designed by the privileged and often for profit, “increases inequality and threatens democracy” (see [Lamb, 2016] for a review). She illustrates with a series of examples ranging from assessment and estimation of teacher quality, recidivism risk, creditworthiness and college rankings to employment application screeners, policing and sentencing algorithms and workplace wellness programs to show that they reinforce inequality and reward the rich and punish the poor. The bias is either present in the algorithm or in the data and sometimes even in both. The common traits of such poor fallout of predictive analytics usually are opacity, scale, and damage. [Thatcher et al., 2016] argue that “As algorithms select, link, and analyse ever larger sets of data, they seek to transform previously private, unquantified moments of everyday life into sources of profit.”

Despite the above risks, because of the enormous benefits that digitisation and analytics promise, they are faits accomplis and the question is only one of realising them safely and well. The *Orwellian big brother* and the *Kafkaesque* arguments certainly raise crucial concerns, but they do not necessarily imply that privacy protection is impossible with digitisation using a unique identifier. Also, despite clearly suggesting that “The technology exists! If we develop the will, we can use big-data to advance equality and justice” [O’Neil, 2016], her work is often interpreted to infer that predictive algorithms are necessarily evil. Such a conclusion, from a few examples of badly done predictive analytics, is overly pessimistic and inductivism at its worst.

3 Analysis of suggested measures

Attempts at privacy protection in digital databases have mainly been based on the tenets of legitimate state interest; informed consent and notice; collection, purpose and storage limitation; participation of individuals; transparency; regulations, enforcement and accountability [The Planning Commission: Government of India, 2011, Srikrishna et al., 2017]. These measures, however, have turned out to be less than effective in preventing a shift to a post-privacy world, at least insofar as personal data is concerned. We try to understand why?

3.1 Legitimate state interest

Clearly, the same privacy protection principles cannot be horizontally applied to the state and other essential bureaucracies, like banking and insurance for example, and to non-essential private digital services where user participation is voluntary. In the first situation the state would most often require the digitisation to enforce *compliance*, such as in income tax. In all such cases the state can mandate digitisation of personal information only after establishing a *legitimate state interest* and enacting a law [The Puttaswamy judgment, 2017, Agrawal, 2017]. All constitutional tests of proportionality, reasonableness and non-arbitrariness would need to be applied. Here, the role of *consent* would be minimal, but *collection* and *purpose limitation* would be important operative principles. However, merely enacting a law would not absolve the state and other bureaucracies from the responsibility of protecting privacy rights of individuals, and all the risks mentioned in the previous section will still have to be mitigated. The state’s understanding of this principle, however, is often questionable.

3.2 Informed consent, notice, purpose limitation and opt-out

For all other cases of voluntary participation, *privacy self-management* [Solove, 2012] through *informed consent* operationalised by effective *notice; collection, purpose and storage limitation; transparency*; and *individual participation* through *opt-in* and *opt-out* have often been advocated as foundational principles for privacy protection [The Planning Commission: Government of India, 2011]. However, as pointed out in [Srikrishna et al., 2017, Solove, 2004, Matthan, 2017], notice and consent are usually ineffective because of information overload, limited choice and *consent fatigue*. In fact, the customary negligent clicking of ‘I Agree’ and the overwhelming burden of information required for informed consent, both in terms of volume and complexity, have made the consent principle impractical for privacy protection. [Matthan, 2017] makes a strong case for a rights-based approach that shifts a significant part of the responsibility and accountability from the individual to the data controller, irrespective of the level of consent. This clearly is required, in addition to consent, and a strong regulatory framework can lay out the standards. However, the methods of enforcement and detection of breaches remain open questions.

Similarly, it may not always be possible to enumerate the purposes for which personal data may be used at the time of collection, and *purpose limitation* is a difficult privacy protection principle to administer [Moerel and Prins, 2015]. In particular, any inflexible implementation of purpose or storage limitation can severely impede innovation in the age of predictive analytics and machine learning where new uses of transactional data and new methods of processing are being discovered every day. Perhaps a combination of *legitimate interest* and purpose limitation under reasonable regulatory control is what is required. However, the regulatory control should not be so lax that it is ineffective, neither should it be so overbearing or paralytic with inertia that it stifles innovation.

Finally, whenever there is a purpose extension not covered by a legitimate state interest, there should always be a notice for consent renewal and an opt-out alternative with a guarantee of deletion of all personal data. It is the recognition and acknowledgement of purpose extensions, however, that have often been problematic.

3.3 Right to explanation

The European GDPR proposes right to explanation as a countermeasure to indiscriminate and biased machine learning applications [Selbst and Powles, 2017]. However, predictive analytics rarely support causal reasoning, and, without expert audit of algorithmic and data biases, the explanations will most likely turn out to be inane. Moreover, the adverse outcomes of perverse machine learning applications are *Kafkaesque*, and the consequent damages are not immediately obvious. So timely explanations may never even be sought.

3.4 Regulation and enforcement

[Srikrishna et al., 2017] propose a strong regulatory framework for enforcement of privacy standards and for fixing accountability. The framework can range from the currently prevailing self-regulation to a more prescriptive “command and control”, and the committee advocates a middle path of co-regulation. However, the approach presupposes that privacy invasions are detectable. The ‘data as property’ view for privacy protection espoused by [Tarafder and Basu, 2017] also assumes the same. This assumption, however, is problematic since detection of privacy infringements, especially of the *Kafkaesque* types, will always be uncertain because the causal effects of invasions will be hard to determine. For example, it may turn out to be impossible to know for sure whether a person has lost her job because her personal medical data was accessed without authorisation and used to discriminate against her, or some other reason put out as the

official explanation was really the determining factor.

We propose instead that the regulatory framework be built into the privacy protection architecture [Agrawal et al., 2017].

4 Elements of an architectural solution

Pivotal to protecting the autonomy of an individual is to protect her identity from getting disclosed when not required, to protect her from unauthorised profiling without her knowledge, and to inform her about all accesses to her data and their outcomes. We contend that the following architectural properties in digital databases are crucial to achieve these objectives.

4.1 Identity protection through virtual ids

Using the same personal identifier for all applications and frontend databases is architecturally unsound from a privacy protection point of view. A straightforward alternative would be to use different virtual identifiers for each application domain, making unauthorised correlation of identities across silos impossible. The mapping between the different virtual identifiers can be maintained securely at a central place with strong access control protocols, and can be used to facilitate legal and authorised mining of personal information across silos [Agrawal et al., 2017]. This would be required not only for a national digital identity, but also for all other unique personal identifiers like the income tax PAN or mobile phone numbers, which have tacitly been converted to unique digital identifiers by the Indian private enterprise. There should be no need to disclose one's real phone number to vendors or for train journeys, and it should be possible to generate virtual and limited duration numbers linked to the original ones on demand. A backend mapping can then route calls and messages to the real ones.

In addition, for effective privacy protection it will be imperative not to use any other weak identifiers like names and addresses in frontend databases. All frontend transactions should store only virtual numeric identifiers after verifying the authenticity using a safe protocol. It is well known that anonymisation with provable guarantees [Dwork, 2011] is hard to achieve in presence of weak identifiers.

4.2 Online regulatory framework for authorisation and access control

Not only are independent regulatory authorities overseeing the data controllers necessary for privacy protection, we argue that the regulatory authorities need to have active presence in the data protection architecture to enable them to prevent privacy breaches from happening. Apart from grievance redress and determining fairness of algorithms and use cases, they need to play two other main roles.

The first role ought to be to determine and clearly define who can access what data and for what purposes, based either on legal sanction or on a consent principle, in conformance with a rights-based data protection law. Purpose limitation needs to be built into such authorisations, and all purpose extensions and consent renewals should be explicitly considered. Such access rights to personal data should not only be defined for operational, investigation and audit purposes, but also for granting algorithmic access for data mining. As [Seth, 2017] points out, despite the recent progress in attempts to build fairness into algorithm design, fairness guarantees are not always possible [Kleinberg et al., 2016]. Hence manual scrutiny and regulatory control of both algorithmic procedures and their use in societal applications are imperative.

Once such access rights are clearly defined and digitally coded, and the authorisations recorded, the second crucial role should be to ensure that data can be accessed only through audited, pre-approved and

digitally signed computer programs after online authentication and verification of the authorisations presented. The regulators should also ensure that the accessed data is used only for authorised purposes by authenticating the genuineness of the accessing programs in real-time. This would require the regulators to audit, approve and digitally sign all programs that data controllers may use to access and process the data. Both the data regulator and the data controller should maintain non-repudiable logs of all data accesses, and neither should be able to access the data independent of the other. Finally, for the sake of transparency, all outcomes of accesses to personal data should always automatically be communicated to the concerned individuals through private channels.

The technology to support such regulatory functions exists (see [Agrawal et al., 2017] for a preliminary analysis), what are necessary now are the will to build the required regulatory capacity and an effective, rights-based data protection law. A co-regulatory approach, where private bureaucracies and data controllers can have their own independent data regulators who can act like online ombudsmen and monitor and enforce privacy protection, can possibly help in building such regulatory capacity faster. Essential state bureaucracies like the national identity or income tax authorities will however require a central data regulatory authority.

5 Conclusions

We have argued that a passive regulatory framework based on detection of privacy breaches, and traditional approach to privacy protection based on the principles of consent, purpose limitation and transparency is unlikely to be successful. In addition to these standard measures we advocate an architectural solution based on online validation of authorisation and access control to prevent privacy infringements in the first place.

Acknowledgement

I thank all students and faculty colleagues who participated in the course on *Digital infrastructure, identity, online data and privacy* held between September and November, 2017 at IIT Delhi. I also thank the guest speakers Usha Ramanathan, Elizabeth Bennett and Arghya Sengupta for their insightful talks in the course. I specially thank Subodh Sharma for his many useful comments on this manuscript.

References

- Kanu Agrawal. Legitimate and Compelling State Interest: The Test for Aadhaar, 2017. URL <https://barandbench.com/legitimate-state-interest-test-aadhaar/>. [Online; posted 31-August-2017].
- Shweta Agrawal, Subhashis Banerjee, and Subodh Sharma. Privacy and Security of Aadhaar: A Computer Science Perspective. *Economic and Political Weekly*, Vol. 52(Issue No. 37), 16 2017.
- Subhashis Banerjee. A Welfare Test for Aadhaar, 2017. URL <http://indianexpress.com/article/opinion/columns/a-welfare-test-for-aadhaar-upa-nda-aadhaar-card-4921582/>. [Online; posted 4-November-2017].
- Gautam Bhatia. The Supreme Court's Right to Privacy Judgment - IV: Privacy, Informational Self-Determination, and the Idea of Consent, 2017a. URL <https://indconlawphil.wordpress.com>.

- [com/2017/08/30/the-supreme-courts-right-to-privacy-judgment-iv-privacy-informational-self-determination-and-the-idea-of-consent/](http://www.nytimes.com/2017/08/30/the-supreme-courts-right-to-privacy-judgment-iv-privacy-informational-self-determination-and-the-idea-of-consent/). [Online blog; posted 30-August-2017; Accessed January 9, 2018].
- Gautam Bhatia. The Supreme Court's Right to Privacy Judgment. *Economic and Political Weekly*, Vol. 52 (Issue No. 44), 04 2017b.
- Nicholas Confessore. Cambridge Analytica and Facebook: The Scandal and the Fallout So Far, 2018. URL <https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html>. [Online; posted 04-April-2018].
- Jean Drèze. The Aadhaar coup. <http://www.thehindu.com/opinion/lead/jean-dreze-on-aadhaar-mass-surveillance-data-collection/article8352912.ece>, 2016. [Online; posted 15-March-2016].
- Cynthia Dwork. The promise of differential privacy. a tutorial on algorithmic techniques. In *52nd Annual IEEE Symposium on Foundations of Computer Science*, October 2011. URL <https://www.microsoft.com/en-us/research/publication/the-promise-of-differential-privacy-a-tutorial-on-algorithmic-techniques/>.
- Jon M. Kleinberg, Sendhil Mullainathan, and Manish Raghavan. Inherent trade-offs in the fair determination of risk scores. *CoRR*, abs/1609.05807, 2016. URL <http://arxiv.org/abs/1609.05807>.
- Evelyn Lamb. Review: Weapons of Math Destruction, 2016. URL <https://blogs.scientificamerican.com/roots-of-unity/review-weapons-of-math-destruction/>. [Online; posted 31-August-2016].
- Rahul Matthan. Beyond Consent: A New Paradigm for Data Protection - Discussion Document 2017-03, July 2017. URL <http://takshashila.org.in/wp-content/uploads/2017/07/TDD-Beyond-Consent-Data-Protection-RM-2017-03.pdf>.
- Lokke Moerel and Corien Prins. On the Death of Purpose Limitation, June 2015. URL <https://iapp.org/news/a/on-the-death-of-purpose-limitation/>.
- Cathy O'Neil. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. Crown Publishing Group, New York, NY, USA, 2016. ISBN 0553418815, 9780553418811.
- Malavika Raghavan. Before The Horse Bolts, January 2018. URL <https://www.thinkpragati.com/think/brainstorm/3180/before-the-horse-bolts/>.
- Andrew D Selbst and Julia Powles. Meaningful information and the right to explanation. *International Data Privacy Law*, 7(4):233–242, 2017. doi: 10.1093/idpl/ipx022. URL <http://dx.doi.org/10.1093/idpl/ipx022>.
- Suchana Seth. Machine Learning and Artificial Intelligence. *Economic and Political Weekly*, Vol. 52(Issue No. 51), 23 2017.
- Daniel J. Solove. *The Digital Person: Technology And Privacy In The Information Age*. New York University Press, New York, NY, USA, 2004. ISBN 0814798462.

- Daniel J. Solove. Privacy Self-management and the Consent Dilemma. *Harvard Law Review*, 126(1880), 2012. URL https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2171018.
- Nova Spivack. The Post-Privacy World, 2013. URL <https://www.wired.com/insights/2013/07/the-post-privacy-world/>. [Accessed January 9, 2018].
- B. N. Srikrishna, Aruna Sundararajan, Ajay Bhushan Pandey, and Others. White Paper of the Committee of Experts on a Data Protection Framework for India, 2017. URL http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_171127_final_v2.pdf. [Online; Accessed January 9, 2018].
- Agnidipto Tarafder and Arindrajit Basu. Taking a fresh guard. *Economic and Political Weekly*, Vol. 52(Issue No. 40), 07 2017.
- Jim Thatcher, David O’Sullivan, and Dillon Mahmoudi. Data Colonialism through Accumulation by Dispossession: New Metaphors for Daily Data. *Environment and Planning D: Society and Space*, 34(6):990–1006, 2016. doi: 10.1177/0263775816633195. URL <https://doi.org/10.1177/0263775816633195>.
- The European Parliament and the Council of European Union. Regulation (EU) no 2016/679, 2016. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679>.
- The London School of Economics and Political Science, 2005. The Identity Project: An assessment of the UK Identity Cards Bill and its implications. <http://www.lse.ac.uk/management/research/identityproject/identityreport.pdf>, June 2005.
- The Planning Commission: Government of India. Report of the group of experts on privacy chaired by Justice A P Shah. http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf, December 2011.
- The Puttaswamy judgment, 2017. K S Puttaswamy v Union of India (2017): Writ Petition (Civil) No 494 of 2012, Supreme Court judgment dated 24 August, 2017. URL http://supremecourtindia.nic.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf. [Accessed January 9, 2018].