The Illusion of Digital Consent

Abstract

Every app, website and online service asks us to agree to something before we can use it, and almost all of us click “I agree” without reading a single line. This article looks at how much that click is actually worth. It compares how seriously we treat consent in real life with how easily it is taken online, and it goes through research showing that people skip terms they would never accept if they read them, that cookie banners are designed to push us towards saying yes, and that even simple apps ask for far more access than they need. It then turns to Pakistan, where a lot of personal data is public before anyone even asks for consent, through exam results, board gazettes and vehicle lookups, and where leaks from national databases end with a few suspensions while the country still has no data protection law. The article argues that consent online has become more of a ritual than a real choice, and it ends with small, practical steps people can take while the bigger fix is still missing.

1. Nobody Actually Reads What They Agree To

Let me be honest first. I have never read a full terms and conditions page in my life, and I am fairly sure you haven’t either. You download an app, a long wall of text shows up, you scroll to the bottom, tick the box and that’s it, done. We call this “consent,” but most of the time we have no idea what we just agreed to.

The strange thing is how seriously we take consent in real life. If someone picks up your phone and starts scrolling through your gallery, you would snatch it back straight away. If a stranger takes a picture of you or your family on the street without asking, people here would actually go and confront him, and honestly it could turn into a whole fight. Even at home, reading someone’s diary or opening their letters is seen as a big line to cross. We grow up knowing that you ask before you look, and you ask before you take.

Online, that whole idea just disappears. When you post a picture on Instagram, you are giving Meta, the company that owns it, a worldwide, royalty-free (free of any payment to you), transferable license to use it. That means they can copy it, show it, change it and even pass that license on to others, and you don’t get a single rupee. Meta has also said that it uses public posts from Instagram and Facebook to train its AI models, and it admitted in an Australian Senate inquiry that public posts from adults going back to 2007 had been used. So the same picture that you would never let a stranger take on the street is being used by a company in ways you never even thought about, and the only “permission” they have is a box you ticked years ago without reading.

This isn’t just a feeling, it has actually been tested. In 2016, two researchers, Jonathan Obar from York University and Anne Oeldorf-Hirsch from the University of Connecticut, made a fake social network called NameDrop. They told 543 university students that their university had been asked to test it before launch. Hidden inside the terms were two ridiculous clauses. One said that NameDrop could share their data with the NSA (the US National Security Agency) and with employers. The other said that, as payment for using the site, users would give up their firstborn child. And 98% of the students missed both of them. On average, the terms of service

were read for about 51 seconds, when they should have taken around 16 minutes to read properly. And these were communication students, people who study this kind of thing.

The funny part is that even if we wanted to read everything, we really couldn't. Back in 2008, two researchers at Carnegie Mellon University, Aleecia McDonald and Lorrie Faith Cranor, worked out that an average privacy policy takes about 10 minutes to read. Then they added up all the websites a normal American visits in a year, and found that reading every privacy policy would take about 76 working days. That was 2008, before most of us had even ten apps on our phones. So when a company says "you agreed to this," the honest answer is that the system was built in a way where agreeing without reading was the only realistic option.

2. The Reject Button Is Hidden on Purpose

You have definitely seen those cookie pop-ups on websites. There's a big bright "Accept all" button, and somewhere below it there is a small grey link that says "Manage settings." If you click that, you get a long list of switches, and sometimes you have to go through two or three screens just to say no. This is not bad design by accident. There's actually a name for it, dark patterns, which means design that quietly pushes you towards the choice the company wants.

In 2020, researchers from MIT, UCL and Aarhus University looked at consent pop-ups on the top 10,000 websites in the UK. Out of the 680 sites using the most popular consent tools, only 11.8% met even the minimum requirements based on European law. They also ran an experiment, and found that just removing the "reject" option from the first screen increased the number of people who said yes by 22 to 23 percentage points.

Think about what that means. Europe actually has strict privacy rules, and companies still found a way to turn "consent" into a game of who gets tired first. Most of us get tired first, click accept and move on with our day. Therefore, the click looks like our choice, but the path to it was decided for us.

3. Why Does a Torch App Need My Contacts?

Apps are even worse, because the permissions they ask for are quieter. When you install something, it asks to access your camera, your location, your contacts, your microphone, and most people tap "Allow" on everything just to get it working.

In 2019, the security company Avast looked at 937 flashlight apps on the Google Play Store. A torch app needs basically one thing, which is access to your phone's flash. And yet these apps asked for 25 permissions on average. Some asked for 77. Out of those 937 apps, 180 wanted to read your contact list, and 77 wanted permission to record audio. Avast's researcher said many of these developers seemed to be running a money-making system, collecting users' data and sharing it with partners. The funniest part is that most phones already have a torch built in, so many of these apps did not need to exist in the first place.

The torch app is just one example, but it shows the pattern pretty clearly. The app gets something simple done for you, and in return it quietly takes much more than the job requires. You "allowed" it, so technically it's all fine.

4. In Pakistan, Nobody Even Asks

Everything so far is about people agreeing without reading. In Pakistan, it goes one step further, because a lot of our data is out there before anyone even asks us to agree to anything.

I'll start with something from my own life. When I checked a result online by entering a roll number, the result page showed the student's CNIC (national ID card) number right there along with everything else. You don't need a password or anything. You only need someone's roll number. On top of that, boards publish result gazettes, which are huge PDF files with the results of every student who appeared. Depending on the board, a record can include the student's name, roll number, father's name and their marks in every subject. News websites then upload all the gazettes together in one place to make it "easier for students." So anyone, anywhere, can open a file and look up a student's name, their father's name and how well they did. Nobody asked those students if they were okay with that.

Boards have also leaked much more than results. In 2016, ProPakistani reported that the Lahore Board was exposing students' names, mobile numbers, addresses, CNIC numbers, fathers' names, school names and even their pictures, including pictures of girls. In 2024, when boards across Pakistan announced their top-performing intermediate students, the names were published along with the students' home addresses and mobile numbers, and female students were especially affected. One parent said her daughter's number started getting random WhatsApp messages after that.

Vehicles are the same story. In Sindh, you can type any number plate into the Excise department's website, and it shows the owner's name along with the car's details. Since 2020, you can even search the other way around, by typing in someone's CNIC number. Guides for the Punjab portal say it shows the owner's name, father's name and city. So if you see a car parked outside a house, you can find out who owns it in a few seconds, and that's the official government system working the way it is supposed to.

Then there is the illegal side. In 2023, Digital Rights Monitor found a website being advertised on a major news platform that let anyone look up Pakistanis' personal data. When they tested it, most searches gave back accurate CNIC numbers and home addresses. Websites like this keep coming back in Pakistan, and nobody seems surprised anymore.

5. When Our Data Leaks, a Few People Get Suspended

The biggest case so far is NADRA (National Database and Registration Authority), the organisation that issues our national ID cards and holds our personal records. After a cyber attack in March 2023, a joint investigation team (JIT) was formed to look into it. In 2024, it reported that the data of 2.7 million Pakistanis had been compromised between 2019 and 2023, allegedly with the involvement of NADRA offices in Multan, Peshawar and Karachi. According to the report, the data moved from Multan to Peshawar, then to Dubai, and was eventually sold in Argentina and Romania. (Some outlets reported this as 27 million, but the JIT figure reported by most sources is 2.7 million, or 27 lakh.)

So what happened after that? More than a dozen NADRA officers faced disciplinary action, and eight of them were suspended and formally charged. From everything I could find, that's pretty much where it ended. I couldn't find any report of the people whose data was stolen being told

about it, and since Pakistan has no data protection law, there was no proper system to fine anyone or force them to inform the victims.

And it did not stop there. In 2025, Dawn reported that a NADRA official and his associate were arrested in Hyderabad by the National Cyber Crime Investigation Agency. They were accused of accessing NADRA records illegally and selling people's data to WhatsApp groups, with the associate sending CNIC numbers and the official sending back the details. So the system we are forced to trust with our most personal details can be leaked by the people working inside it, and sold through an app most of us use to send good morning messages to our relatives.

6. There Is Still No Law to Protect Us

Our Constitution, in Article 14, says that the dignity of man and, subject to law, the privacy of home shall be inviolable (cannot be violated). The Supreme Court, in the Benazir Bhutto case, even read this broadly and said that a person's privacy goes with them wherever they live or work, and not just inside the four walls of their house. That sounds good on paper. But when it comes to digital data, Pakistan still does not have a proper data protection law. A draft Personal Data Protection Bill was first prepared in 2018. Since then there have been new drafts, new deadlines and new promises, and as of September 2026 it still has not been passed into law. There is also no independent authority whose actual job is to protect our data. The little that exists falls under PECA (the Prevention of Electronic Crimes Act), and enforcement goes to the FIA and PTA.

This is where the whole idea of consent breaks down for us. In Europe, at least, companies can be fined when they misuse data, even if many of them still play games with cookie banners. Here, if a board puts your CNIC on a result page or someone sells your address on a website, there isn't really a clear law to point to or a clear office to complain to. Therefore, our "consent" is not just ignored, there's nothing standing behind it in the first place.

7. What We Can Actually Do

I won't pretend that one person can fix this, because the real fix is a proper law with someone actually enforcing it. But there are still a few small things we can do so that we are not making it easier for anyone.

Start with your phone. On Android, go to Settings, open Apps, pick an app and look at its permissions. If a game or a torch app has access to your contacts or microphone, turn it off. Use the torch that's already built into your phone instead of downloading one. When a website shows a cookie pop-up, take the extra five seconds to find "Reject all." It's annoying, I know, but that annoyance is exactly what they are counting on. And before posting pictures of your family publicly, think about whether you'd be okay with a stranger having them, because in a way, a company now does.

Be a little careful with your CNIC too. We hand out photocopies of our ID card everywhere, to shops, SIM sellers, landlords, without asking where the copy goes afterwards. You won't be able to avoid it every time, but you can ask, and you can write on the copy what it is for. And

when people talk about data protection, add your voice to it, because the bill has been sitting there for years, mostly because not enough of us seem to care.

The next time you click “I agree,” just notice it for a second. That click is supposed to mean you made a choice. For most of us, most of the time, it really doesn’t.

References

1. Instagram Terms of Use license and Meta AI training: WKYC Verify; The Conversation, Ten things you should know about Instagram’s terms of use; HuffPost UK, Australian Senate inquiry
2. Obar, J. A. and Oeldorf-Hirsch, A. (2016). The Biggest Lie on the Internet. Coverage: Sophos; WBTV; NPR
3. McDonald, A. M. and Cranor, L. F. (2008). The Cost of Reading Privacy Policies. Paper PDF; Benton Institute summary
4. Nouwens, M. et al. (2020). Dark Patterns after the GDPR. MIT DSpace
5. Avast (2019) flashlight apps study: SecurityWeek; Avast Decoded
6. Result gazettes: ProPakistani, BISE Multan gazette (2026); Daily Pakistan, BISE Rawalpindi gazette (2026); ProPakistani, all Punjab BISE gazettes (2022)
7. ProPakistani, Lahore Board is Exposing Private Data of All Students (2016)
8. ProPakistani, Intermediate Students’ Addresses and Phone Numbers Leaked by Boards Across Pakistan (2024)
9. Vehicle lookups: PhoneWorld, Vehicle Verification in Sindh; Zameen, Sindh verification by CNIC; Zameen, Punjab verification guide
10. Digital Rights Monitor, Illicit website offering CNIC data advertised on news platform (2023)
11. NADRA JIT report: ProPakistani (2024); suspensions: Pakistan Today (2024)
12. Dawn, NADRA official arrested for selling data to WhatsApp groups (2025)
13. Article 14: Constitution of Pakistan, Part II Chapter 1; Benazir Bhutto case reading: Dawn
14. Data protection law status: Digital Pakistan (Oct 2026); RecordingLaw, Pakistan Data Privacy Laws 2026