The government's priority is to access our personal data—not protect it

THE SOUND & THE FURY

Sushmita S Preetha
is op-ed editor at The Daily Star.

SUSHMITA S PREETHA

Are we really all so nonchalant about the fact that our personal data is up for grabs?

Following multiple cybersecurity fiascos earlier in the year, including the leak of Smart NID Card information of at least 50 million Bangladeshis, the tech magazine *Wired* has uncovered another disturbing instance of data breach—this time from the database of an intelligence agency in Bangladesh. As per the report, the National Telecommunication Monitoring Center (NTMC) left exposed sensitive personal information for months on end through an unsecured database on its system. The breached data include the names, professions, blood groups, parents' names, phone numbers, call durations, vehicle registration information, passport details, fingerprint photos, personal financial details, national ID numbers, and so on—basically all the metadata that dictates and describes our online (and, by extension, our offline) lives. While some of it was test data, the *Wired* could verify a sample of real-world names, phone numbers, email addresses, locations, and exam results.

But let's pause for a moment and ask: why does the NTMC have the data to begin with?

The NTMC is a national-level intelligence agency of Bangladesh responsible for monitoring, collecting, recording, and the interception of electronic communication such as phone calls, emails, and social media accounts. Reconstituted as an independent agency in January 2013, from the previous National Monitoring Centre established in 2008, the NTMC has been drastically empowered in recent years to monitor people's personal communication—under the orders of the government of Bangladesh.

Beyond information that we willingly share with various government agencies, such as national ID or passport details, the breached data from the NTMC database also contains such information as which numbers a person may have called and for how long, and the amount of money in their bank accounts. The *Wired* investigation stated that it was "unclear why the data has been collected, where it has all been collected from, or what it is being used for," concluding that there is "no indication that it relates to any wrongdoing."

The NTMC's mission and objective state that it monitors, collects, and records data "lawfully." But who gets to decide what is and isn't lawful if not the all-powerful government, in the absence of any judicial oversight? What mechanisms are in place to ensure that they don't overextend themselves in pursuit of their own political agendas and interests, and in violation of people's right to privacy? Our constitution guarantees the rights to privacy, freedom of speech, thought and conscience as well as the right to life and personal liberty, but it also allows for "reasonable restrictions imposed by law... in the interest of national security" under Article 43. As per Section 46 of the ICT Act (2006), the government may intercept data in the interest of the sovereignty, integrity or security of Bangladesh, friendly relations of Bangladesh with other States, or public order—but what each of these terms mean, as we all know by now, is open to (mis)interpretation.

VISUAL: **ANWAR SOHEL**

The NTMC's mission and objective state that it monitors, collects, and records data "lawfully." But who gets to decide what is and isn't lawful if not the all-powerful government, in the absence of any judicial oversight? What mechanisms are in place to ensure that they don't overextend themselves in pursuit of their own political agendas and interests, and in violation of people's right to privacy?

We have known for some time now—thanks to investigations by credible international news outlets and watchdogs—that the government has been buying advanced spyware, including from Israeli cybersecurity companies, to snoop on its citizens. In a telling move, the High Court rejected a writ petition that sought its directive on the government to take necessary steps to prevent eavesdropping and recording of private phone conversations in September 2021. In January this year, the government went one step further in legalising their surveillance mechanisms, when home minister Asaduzzaman Khan declared that they will soon introduce an Integrated Lawful Interception System (ILIS) to monitor social media and thwart various "anti-state and anti-government activities." The government, which had wanted to introduce this system ahead of the elections in 2018, is reportedly deploying it ahead of the upcoming general election. Purchased with $2 billion, the ILIS enables law enforcement and intelligence agencies to access the precise location as well as other confidential information of a mobile phone user.

Alarmingly, the telecom companies are legally obligated to participate in such gross violations of the privacy and human rights of their users. According to Section 97(A) of the Bangladesh Telecommunication Regulatory Act, telecommunications companies are bound to obey any order from the government to prevent, record, and collect information of any message or voice call of any user of telecommunication services "for the sake of the state's security or public order." More incredibly still, the money required for procuring and installing the surveillance software and equipment will reportedly have to be borne by the companies themselves—which means, in the end, it is the consumers who will end up paying for their own surveillance.

It's astonishing to think how easily the government has managed to pull all this off. At a time when opposition activists and leaders are indiscriminately being arrested and picked up from their homes and other locations, we can well imagine how such surveillance mechanisms are being used to that end. And it's not just the opposition whose geolocations are at stake. Once such a system is instituted, there is nothing to stop the authorities from using it to monitor and locate anyone they consider a threat, and from the way journalists, students, and academics have been arrested under the Digital Security Act, we can conclude that the range of who they deem a criminal is quite broad and arbitrary.

The government has made it clear that when it comes to our private data, its priority is to get access to it by any means—but not protect it. It has heavily invested in purchasing surveillance equipment and enhancing the capacities of various agencies to use them over the years. Unfortunately, though, the government has not even shown an iota of the same interest in what should have been its priority—protection of citizens' data—as proven time and time again by the numerous data leaks and hacks in this year alone. When data breaches take place from the server of the Office of the Registrar General, Birth and Death Registration (BDRIS)—one of the 29 government-declared critical information infrastructures—or that of an intelligence agency—which is supposed to have the most advanced cybersecurity measures in place—it becomes obvious just how vulnerable Bangladesh's whole IT infrastructure is. We are so ill-equipped, in fact, that our agencies can't even bring themselves to respond or react to emails from foreign cybersecurity experts pointing out the leaks on time. Despite the severity of the breaches and the implications they have for the citizens involved, our authorities are yet to hold accountable the agencies in question or take any meaningful steps to bolster their cybersecurity measures.

The government's failure to protect our data is a violation and crime all on its own, for which we, as citizens, should be able to hold it responsible. Unfortunately, avenues for us to sue the government for such breaches do not yet exist. One could have looked to the proposed Data Protection Act for redress in the near future, but in its current form, the bill—even after the removal of the indemnity clause which provided authorities immunity from criminal and civil liability—is an exercise in enhanced surveillance rather than protection. Its insistence on data localisation—requiring all companies operating in the country, including Facebook, Google, Whatsapp, etc, to store their data in the country—would not only mean that the government can access our private data anytime they want on pretexts of national security, law and order, friendly relations, etc, but also makes us sitting ducks for hackers, given the country's proven poor track record.

The problem with an undemocratically elected government is precisely that it is accountable to no one. Whether it is stealing our data, snooping through it, or failing to protect it, citizens seem to have very little say in the matter. And it doesn't help that we would rather just watch reels on social media than worry about who is reading our emails, tracking our location, or accessing our bank details—and, in the process, making a mockery of our democratic and human rights.

AI is the printing press reborn

Shakil Rabbi
is an assistant professor at Virginia Polytechnic Institute and State University. He studies how rhetoric, languages and writing shape our social lives. Reach him at ssrabbi@gmail.com

SHAKIL RABBI

There is a lot of hand-wringing going on nowadays about literacy. People are worried about how we can teach students productively, given that artificial intelligence can pass most tests or assignments. How are we to interpret students' abilities, or even know that what we are reading was composed by a thinking human being who possesses morality and accountability? While the reason behind these anxieties is novel, the tradition of moral panic when it comes to writing is not. As long as people have been writing, people have also been complaining about how it undercuts our humanity. It is in this context that we need to understand generative AI and what it represents as a technology.

When we see writing as a vehicle for something (such as thinking), AI becomes akin to a calculator. But when we think of writing as an end in itself (such as a perfect essay), we become completely unprepared for what is to come. All through history, transformations around technologies of literacy have usually led to revolutionary changes across societies—because we are so deeply organised by the written word.

Being suspicious of writing technologies

Writing was invented in ancient Mesopotamia to keep records. People soon also understood its power as discourse—a way of speech—that went beyond bean-counting; and so we began writing down stories, poems, and prayers. People started to believe that it was a gift from the gods, an act of compassion from the divine that was also a curse. An ancient Egyptian myth goes that the god Thoth gave writing to men as an aid for memory. King Thamus, learning what writing could do, concluded that it would rob people of understanding, given that mankind is lazy and would stop learning things because they could not always fall back on what was written.

VISUAL: **REHNUMA PROSHOON**

Plato, in *Phaedrus*, compared writing to painting and said that, like images, the written word cannot respond to questions. "It is the same with the written words," Plato ventriloquised through Socrates, "they seem to talk to you as though they were intelligent, but if you ask them anything about what they say, from a desire to be instructed, they go on telling you just the same thing forever. It provides an image of truth with truth." The theme is the same as when a tool to make things better actually makes things worse because of how people use it.

But we know that these warnings against writing were false. In fact, we have progressed in ways the ancients cannot even fathom. We have gone to the moon, and we have cured a disease such as smallpox, hopefully forever. Our moral senses have also improved. For example, slavery, common for so long, is now beyond the pale. This is not to say that we are innately better; our darker natures continue to stalk us, and we still explode with unbelievable cruelty, apathy, and greed, through acts small and universal. And through it all, writing has been there: scientists relied on writing to work together on vaccines and Nazis kept famously detailed ledgers of the people they sent to death camps.

Changes in writing technologies

While its impact is subtle, it is irrefutable that the printing press was the bedrock of the modern world. Nation states, the scientific method, Western imperialism, and modernity itself would not exist without moveable print. The printing press allowed for the mass production of written materials, which then led to wide-scale literacy and the spread of knowledge. Mass media, such as newspapers, radio, and television, further accelerated the flow of information and helped create a more informed public and organised modernity. At the same time, if Europe had normalised mass literacy through the printing press, the Enlightenment and European imperialism it engendered would likely have never happened.

The technology of the printed word did this. Empires such as the Ottoman or the Qing dynasty were not able to make use of moveable print in the same way—the quirk of the modular Latin alphabet made it a perfect fit for moveable type—and their mighty societies were superseded and then colonised.

Thinking in writing technologies

So, what does this history mean as we countenance generative AI, stupefied and confused about what it means for our societies that are organised around writing? Our schools won't work if we can't use writing in them. Specifically, we believe we won't know what is being learned if we can't use writing to test it. "Students will cheat," we throw up our hands, "because students are lazy."

AI is an impossible problem if you think of writing as the end. If you think our goal is getting students to produce a text that is correct and marks educatedness, I'm sorry to say that this is now impossible to guarantee in the school setting.

Teachers might ask students to write out answers by hand in exact booklets, but that would mean robbing them of learning how writing functions in the world. The educated need to write in print or digitally, and students won't learn how if writing in school means only writing by hand. Some have also suggested that we assign essays as homework and then ask students questions on their composition. This won't work because students could just ask AI to compose the texts and then read those texts to prepare their answers. It would just double our work, without stopping any student wanting to use AI to compose their assignments.

This problem of AI and writing, however, disappears if we think about writing as a means to an end. AI can write generic compositions on ideas well enough; but it cannot compose specific, task-based texts regarding real world situations. Any writing by AI, after all, is not a real thing, but a simulacrum of real speech. Furthermore, the longer I use AI tools, the clearer it becomes to me that while AI can compose sentences and paragraphs cohesively and correctly, its overall compositions are incoherent. AI writing is unthinking writing—because AI *can't* think. Like Plato's picture, it will just keep telling you the same thing again and again, forever. Given the nature of large language models, it cannot be otherwise.

So, writing as a form of thinking and a way to engage with the world is safe, and will remain so. Furthermore, AI's capacity to parse information quickly and act as a tool to help us think is immensely useful to the task of writing. We should teach students to use it and show them that AI can't actually write, but it can help us read and help us think, which in turn will help us write better. We can now jot down our ideas and use AI tools to get suggestions on how we might develop them further. We could use AI to read difficult texts and understand them better. We can provide an AI tool with our own drafts and ask for ways to build on what we have written (considering its suggestions as a thread to start brainstorming with, rather than as correct feedback.)

Artificial intelligence is the printing press reborn. We need to teach its uses to our students the right way and learn how to adapt to the new context it represents. If we don't master this tool, we risk being unprepared for the new technological world that is approaching us apace.