Policy reset for a digital economy

Privacy, security, portability, and sandboxes

IKBAL HASAN

Barrister Ikbal Hasan is a specialist in corporate and technology law, with a refined understanding of technology policy and regulatory landscapes.

ILLUSTRATION: ZARIF FAIAZ

SUMMARY

1. Bangladesh's digital policy is now an economic rulebook that shapes trust, investment, productivity, and inclusion.
2. A credible reset rests on four linked pillars: privacy, security, portability, and regulatory sandboxes.
3. Privacy should be built into product design through minimisation, purpose limits, retention discipline, youth protection, and workable cross-border safeguards.
4. Security must cover both infrastructure and people, including fraud, impersonation, harassment, misinformation, and synthetic content risks.
5. Portability and interoperability can strengthen user agency and competition, while sandboxes help regulators and innovators test AI-era products under strict, time-bound guardrails.

Bangladesh is approaching a moment when digital policy will increasingly determine economic outcomes. Artificial intelligence has sped up the integration of data, software, and online distribution into every sector, from retail and manufacturing to education, finance, and logistics. In parallel, the creator economy and small business digitisation have expanded rapidly, with more people earning, learning, and building networks through online platforms. In this environment, "digital economy policy" is no longer a specialised topic. It is the rulebook for trust, investment, productivity, and inclusion.

A constructive policy reset can be organised around four pillars that are now standard in mature digital ecosystems: privacy, security, portability, and regulatory sandboxes. These pillars are interdependent. Privacy shapes legitimacy. Security protects people and systems. Portability strengthens user agency and competition. Sandboxes create a structured way to learn and adapt as technology evolves. Together, they support innovation without sacrificing accountability.

PRIVACY AS AN EVERYDAY USER EXPERIENCE

Privacy is often treated as a legal construct defined by notices and consent. But for ordinary people, privacy is experienced through design. It is the ability to understand what is happening, make meaningful choices, and trust that those choices will be respected. Large consumer platforms that operate at scale have learned that privacy cannot rely on paperwork alone. It must be embedded in product architecture through clear settings, intuitive controls, and sensible defaults.

A practical privacy approach begins with data minimisation. Services should collect what is needed for a defined purpose and avoid gathering data simply because storage is cheap or future use is imaginable. Minimisation reduces risk and strengthens public confidence. It also makes compliance simpler for startups and smaller firms by narrowing what must be protected, monitored, and governed.

Purpose limitation follows naturally. When a user provides information for one function, that information should not quietly migrate into unrelated uses. This is where transparency must be clear and specific. Explanations that ordinary users can understand, delivered at the moment a feature is activated, are more effective than lengthy documents few people read. Privacy controls should also be easy to find, easy to change, and consistent across devices.

Retention discipline is equally important. Keeping personal information indefinitely increases the impact of breaches, insider misuse, and operational mistakes. A healthy digital economy encourages retention schedules that match business needs and public expectations, especially for sensitive categories of data.

Youth protection deserves a distinct lens. Bangladesh's demographics make it essential that digital services offer age-appropriate experiences, including stronger default settings for teenagers, additional friction for risky interactions, and tools that help families support safer online habits. These measures are not about limiting opportunity. They enable young people to participate in digital life, build skills, and create economic value with greater confidence.

Privacy must also be designed for a world of cross-border services. Bangladesh's entrepreneurs rely on global cloud infrastructure, cybersecurity services, payment partners, and international customer support tools. Cross-border data handling can be compatible with strong protection when accountability is clear, safeguards are enforced, and responsibilities are well defined. The objective should be to protect people while enabling legitimate digital trade and modern security operations that often depend on global threat intelligence.

SECURITY AS RESILIENCE, INTEGRITY, AND CONSUMER PROTECTION

Security in the AI era extends beyond protecting servers and networks. It includes fraud, impersonation, account takeovers, online harassment, and coordinated deception. It also includes the integrity of information, particularly as synthetic media becomes easier to generate and distribute. A credible security pillar must therefore protect both infrastructure and people.

At the operational level, the strongest security cultures are layered. They include secure engineering practices, continuous monitoring, strong account protections, and tested incident response procedures. Many major platforms also rely on security research engagement and vulnerability reporting channels to identify issues early, and they conduct regular internal and external assessments. These are pragmatic approaches shaped by experience: at scale, security is a constant process, not a one-time certification.

From a policy perspective, security works best when expectations are risk-based and proportionate. A payment provider, a hospital system, and a small ecommerce shop do not face the same threat profile. But every organisation that handles personal information can meet baseline practices such as access control, secure authentication, appropriate encryption, logging, vulnerability management, and incident readiness. When such baselines are widely adopted, the number of preventable failures falls and trust rises across the market.

Security also depends on tackling scams and deception. Online fraud often succeeds through social engineering rather than technical sophistication. The most effective responses combine enforcement against malicious networks with consumer education. Platforms can disrupt coordinated actors, remove impersonation attempts, and reduce exposure to suspicious behaviour. Banks, telecom operators, and consumer protection bodies can reinforce this by sharing threat patterns and supporting victims. A coordinated ecosystem approach lowers the cost of security for everyone and reduces harm at scale.

Integrity in digital spaces is now part of national economic resilience. When manipulation, misinformation, and harassment drive people offline, the costs are social and economic. Responsible platforms invest heavily in moderation, detection tools, and user reporting systems, supported by clear rules and appeals mechanisms. Transparency reporting, when done consistently, helps build confidence by showing how safety and enforcement operate in practice. These mechanisms should be recognised as part of the broader security conversation, not a separate debate.

AI raises a further requirement: clarity around synthetic and manipulated content. As generative tools become mainstream, the digital economy benefits when consumers have signals that help them judge what they are seeing. Labelling, provenance indicators where feasible, and enforcement against harmful deception can reduce the risk that trust collapses under a flood of convincing fakes.

PORTABILITY AS USER AGENCY AND PRO-COMPETITION INFRASTRUCTURE

Portability is sometimes discussed as a technical feature, but its real significance is economic. Portability strengthens user agency, reduces lock-in, and supports competitive markets where startups can challenge incumbents on quality, safety, and innovation. It also reinforces privacy by making control tangible rather than theoretical.

In practice, many large consumer services already provide mechanisms for users to access and download certain categories of account data. They also provide settings that let users manage profile visibility, interactions, and personal information. These capabilities demonstrate that portability can be implemented at scale while maintaining security safeguards.

For Bangladesh, portability can play several roles. It can increase consumer confidence among first-time digital users who worry about being trapped in one service. It can support entrepreneurship by making it easier for small businesses and creators to manage their digital presence and records. It can also contribute to healthier competition by lowering barriers for new services that offer better outcomes for users.

Portability must be designed safely. If the transfer of data is poorly secured, it becomes an avenue for fraud, coercion, or unauthorised access. Safe portability requires strong identity verification, clear user consent, limits on scope, and secure transfer methods. It also benefits from common standards so that portability is usable, not symbolic. Standards reduce friction for startups and allow regulators to supervise more effectively because expectations are consistent.

Interoperability is the natural extension of portability. In a growing digital economy, the biggest productivity gains come when services can connect securely and with permission, whether across payments, logistics, identity verification, or small business tools. Interoperability should be consent-driven, auditable, and limited to defined purposes. When done right, it expands opportunity without turning the ecosystem into an uncontrolled data-sharing environment.

SANDBOXES AS A DISCIPLINED WAY TO LEARN FASTER THAN TECHNOLOGY CHANGES

Even the best-designed policy can struggle to keep pace with AI-enabled products that evolve on quarterly cycles. Regulatory sandboxes offer a practical response: a structured method to test innovation under real conditions with clear guardrails. Sandboxes are sometimes misunderstood as relaxed regulation. The opposite is true when they are designed well. A credible sandbox is rigorous, time-bound, and evidence-driven.

Many responsible digital services already deploy new features through controlled rollouts, monitoring, and iterative improvements, especially for safety-sensitive changes. A sandbox applies similar discipline at the policy level. It creates a setting where regulators, innovators, and stakeholders can observe outcomes, measure risk, and refine safeguards before mass deployment.

For Bangladesh, sandboxes can be particularly valuable in areas where AI promises high public benefit and complex risk, including education technology, health-related services, financial tools, and digital identity adjacent services. Sandboxes can test not only products, but also governance measures such as impact assessments, bias testing, security controls, grievance mechanisms, and transparency practices. They can also help build institutional capability by exposing regulators to real-world systems rather than theoretical models.

A strong sandbox model should protect users explicitly. Participation should be voluntary with clear disclosure. The scale should be limited. The duration should be fixed. Reporting should be mandatory. Exit pathways should be clear, including conditions for scaling, conditions for modification, and conditions for stopping. When these elements are in place, sandboxes reduce uncertainty for investors and innovators while improving consumer protection through earlier, more informed oversight.

A COHERENT RESET THAT SUPPORTS GROWTH AND TRUST

The strategic objective for Bangladesh is not simply to adopt new technologies. It is to build a digital economy that can grow without recurring crises of trust. In an AI-shaped world, trust is a competitive advantage. It attracts investment, supports entrepreneurship, and keeps citizens engaged in digital services that can expand opportunity.

Privacy, security, portability, and sandboxes are most effective when treated as a single system. Privacy builds legitimacy and makes participation sustainable. Security protects people, commerce, and resilience. Portability strengthens user agency and market dynamism. Sandboxes accelerate learning and improve governance quality without freezing innovation.

Bangladesh's youth, creators, and startups are ready to compete in the economy of the future. A policy reset rooted in these pillars can ensure that the digital marketplace remains open, trusted, and resilient, enabling innovation to scale responsibly and inclusively.