AI Governance and Data Minimization in the 5G Era: What Employers and Providers Must Consider Now

Insights
7.30.25

As 5G connectivity becomes more widely deployed, organizations across all industries are leaning into AI tools that promise speed, automation, and deeper insights. But the combined power of 5G + AI creates an urgent compliance imperative: aligning AI governance practices with strong data minimization principles. This insight explains why data minimization – an often overlooked privacy requirement – is foundational to AI risk management and outlines key considerations for employers and technology providers.

The 5G-AI Feedback Loop: Faster Networks, More Data, Greater Risk

5G enables vast increases in data transmission speed, device density, and edge computing. These features allow AI systems to ingest and act on real-time data from endpoints such as employee devices, facility sensors, customer-facing apps, and connected equipment.

But with faster pipelines come expanded exposures. Many AI systems rely on continuous, granular data collection to maintain functionality. If left unchecked, these inputs can exceed what's legally permissible, ethically justifiable, or even operationally necessary.

Regulators are increasingly scrutinizing this dynamic. Agencies such as the FTC, European Data Protection Board, and California Privacy Protection Agency have signaled that data minimization – limiting collection of personal data to what is "adequate, relevant, and necessary" – is necessary with AI deployments.

Why Governance Frameworks Must Include Data Minimization

AI governance policies typically emphasize accuracy, explainability, and bias mitigation. However, few explicitly integrate data minimization as a core principle. That's a problem, particularly in environments powered by 5G, where data flow is constant and instantaneous.

Failure to implement minimization controls can lead to:

- **Regulatory exposure** under laws like the European Union's General Data Protection Regulation (GDPR), the California Consumer Privacy Act/California Privacy Rights Act (CCPA/CPRA), and a growing patchwork of US state privacy laws.

- **Increased data breach risk** due to the unnecessary retention of sensitive data.
- **Litigation risk** from employees, consumers, or other stakeholders alleging excessive surveillance or opaque data use.
- **Operational inefficiency**, as over-collected data introduces noise into AI decision-making and burdens downstream security controls.

5 Practical Steps to Align AI Governance with Data Minimization

To bridge this gap, organizations developing or deploying AI systems – especially in 5G-enabled environments – should incorporate the following steps into their governance programs:

1. Conduct a Data Mapping and Justification Exercise. For each AI system or use case, identify what data is collected, its source, and whether it is strictly necessary to achieve the stated business objective.

State risk flag: Under California's CCPA/CPRA, businesses must disclose the purpose of each data category collected and allow users to limit the use of sensitive personal information. Similar purpose limitation and notice requirements now apply in Colorado, Connecticut, Virginia, and Texas.

2. Integrate Privacy and Security by Design at the Edge. Devices, sensors, and apps operating on 5G networks should include local filtering and anonymization capabilities to prevent excessive upstream transmission.

State risk flag: Colorado's Privacy Act explicitly requires data controllers to implement data minimization and privacy-by-design principles at the system level.

3. Build Minimization Into Model Training and Outputs. AI systems should be designed to minimize reliance on sensitive attributes (e.g., biometrics, location, behavioral profiles) and to limit retention of training data where possible.

State risk flag: Illinois' Biometric Information Privacy Act (BIPA) imposes strict limitations on biometric data collection and retention, with private rights of action. Employers using 5G-connected AI for timekeeping or access control must take particular care.

4. Update Governance Frameworks to Address Real-Time Risk
Include policies for data lifecycle management, employee monitoring, algorithmic review, and vendor oversight tailored to 5G's real-time environment.

State risk flag: New York and California have heightened scrutiny on algorithmic employment decision tools (AEDTs), especially where real-time monitoring or automated profiling is involved. Audit and transparency obligations may apply.

Audit and transparency obligations may apply.

5. Train Cross-Functional Teams

Legal, IT, HR, and operations teams must understand how AI and 5G interact – and what controls are required to stay compliant and mitigate risk.

Conclusion

For support in evaluating your AI governance program, assessing vendor risk, or preparing for AI and data minimization compliance under evolving US privacy laws, please contact your Fisher Phillips attorney, the authors of this Insight, or any member of Fisher Phillips' Data Protection & Cybersecurity or Artificial Intelligence teams. Make sure you are subscribed to Fisher Phillips' Insight System to receive the most up-to-date information directly to your inbox.

Related People

Daniel Pepper, CIPP/US
Partner
303.218.3661
Email

David J. Walton, AIGP, CIPP/US

Partner
610.230.6105
Email

Service Focus

AI, Data, and Analytics

Privacy and Cyber

Data Protection and Cybersecurity

Counseling and Advice

Industry Focus

Tech

Related Offices

Irvine

Los Angeles

Sacramento

San Diego

San Francisco

Woodland Hills

New York

Chicago

Denver