Transparency Battles

Summary: Transparency is increasing, for companies, governments, and individuals, and is in conflict with needs for privacy and secrecy. In a more transparent world, organizations will face a growing expectation of openness and accountability in their decision-making, relationships, and practices.

Forecasts

- Growing demands for organizational transparency will increasingly conflict with security requirements. Managing this tension will require ethical decision-making, public accountability, and granular control over access to information.
- Organizational data leakage and the insights generated from data aggregation poses a growing challenge to information security. Organizations will need to adapt to operating with greater transparency, or undertake more active measures to preserve opacity.
- Social media is an increasingly potent intelligence source for gathering information via the activities and posts of an organization's employees, contractors, and partners. Organizations will need to take a more active approach to balance personal needs for constant connectivity with organizational security needs.
- Growing middle classes in emerging economies will increasingly demand transparency from their governments and companies. Transparency will create new expectations that corruption be curbed, and organizations be more accountable.

Key uncertainties for the future of transparency:

- Shifting desire for privacy vs. security
- Potential public backlash over corporate or governmental privacy abuses
- New regulations to protect individual privacy against data aggregation
- New transparency and disclosure requirements for companies and organizations
- Adoption rate of "ethical consumption" by mainstream consumers

Supporting trends

Politicized commerce. Political polarization is spilling over into commerce, with companies increasingly taking sides on divisive political issues.

Ethics and transparency. Growing transparency spotlights organizational ethics, and is increasing the expectations for public scrutiny of organizational practices.

Smart surveillance. Smart surveillance systems are able to use sensor-fusion technologies to track shoppers picking specific products off shelves in real time.

Concern about online privacy. Consumers are very worried about the privacy of their personal data online.

Data trail control. People are generating vast trails of personal information, leading to growing questions about who should own and control that data.

Accountable AI. Accountability and transparency technologies for machine learning are making it easier for humans to understand the decision-making of AI systems and neural nets.

Consumers love encryption. Strong consumer trust in encryption will continue to make it difficult for law enforcement and government to build back doors into systems for security purposes.

Fears of technology. Polls show that people are afraid of a variety of technological developments, such as cyberterrorism, identity theft, and government tracking of personal data.

Data points

***Transparency and behavior*.** Researchers studied the impact of issuing body cameras to 1,000 police officers in Washington DC, using another 1,000 officers as a control group. The study found no statistically meaningful differences in police behavior between the two groups. While the cameras did not impact behavior, their impartial recording of police interactions with the public can help to boost public trust.

Data growing exponentially. According to InsideBIGDATA, digital information is growing exponentially, doubling in volume every two years. Human and machine data is growing 10 times faster than traditional business data, and sensor data has a growth rate that is 50 times greater.

Topics for additional research

- Legal and societal requirements for balancing data collection and analysis vs. privacy
- Global variations in cultural expectations regarding transparency, accountability, and corruption

Strategic insights

For the security industry

- Security professionals will increasingly need to balance the legal demands of disclosure and transparency mandates with the business requirements of competitiveness. Effective balance between these needs may require security professionals to deepen their understanding of both the legal and business issues adjacent to security practices.
- The security industry will sit between demands for unlimited security and fears about excessive surveillance and tracking. Best practices for data protection and privacy may need to evolve to encompass what data should not be collected or stored.
- The security profession could play a growing role in not just protecting organizations from hacking, but managing their "data profiles" to shape how they are viewable from the outside.
- Social media offers new tools to monitor for organizational security threats but also offers the potential to detect real-time shifts in public sentiment. Collaboration could give security professionals a greater role in internal marketing, PR, and strategy discussions.
- There is growing demand for services that can assist individuals to manage their transparency and preserve a desired level of privacy and security.

For ASIS

- ASIS can help organizations manage global variations in the cultural expectations for transparency and security in organizations.
- ASIS can promote transparency awareness by developing case studies, standards, and best practices for managing organizational transparency.
- ASIS can foster discussions about the ethical tensions between transparency expectations and security requirements.

Timing

- **Stage**: Growing, in a period of expansion
- **Speed**: Moderate, and likely to be influenced by headline events

Potential alternative futures

- **Radical transparency:** Growing demands from the public for institutional accountability push organizations to embrace and expand transparency practices.
- **Ubiquitous blockchain:** The spread of blockchain technologies accelerates the adoption of transparency across business sectors.
- **Owning your data:** Individuals are given much more legal control over their personal data.
- **Hacker insurgency:** Global dissemination of sophisticated hacking tools forces organizations to accept regular hacks and leaks of data as the new normal.