DATA PRIVACY

Privacy

- Privacy is a fundamental human right
  - Underpins human dignity
  - Enables other rights such as freedom of association and freedom of speech
- Several aspects
  - Our focus: Data privacy

Right to Privacy

- Some question that humans have a right to privacy
- Historical protections

Biblical Examples and Principles

- Privacy is part of God's nature

  "The secret things belong to the LORD our God, but the things revealed belong to us and to our children forever" Deuteronomy 29:29

- Jesus taught us to keep our generosity and personal prayers private

  "But when you give to the needy, do not let your left hand know what your right hand is doing, so that your giving may be in secret. Then your Father, who sees what is done in secret, will reward you." Matthew 6:3, 4

  "But when you pray, go into your room, close the door and pray to your Father, who is unseen. Then your Father, who sees what is done in secret, will reward you." Matthew 6:6

Biblical Examples and Principles

- The world often uses privacy as a shield behind which to hide wicked plans and actions.
- Scripture gives guidance for how to protect the privacy of our brethren when wickedness is involved:

  "And if your brother sins, go and reprove him in private... . But if he does not listen to you, take one or two more with you ... . And if he refuses to listen to them, tell it to the church." Matthew 18:15-17
- As professionals and Christians, we have a moral responsibility to create systems that properly safeguard the information entrusted to them by users.

Protecting Privacy

- Approaches:
  - Comprehensive laws
  - Sectoral laws
  - Self regulation
  - Privacy technology

Privacy Legislation

- US
  - HIPAA (1996)
  - COPPA (1998)
  - Sarbanes-Oxley (2002)
  - FACTA (2003)
- European Union
  - GDPR (2016)

Sarbanes-Oxley

- Affects organizations that are publicly owned
- Requires procedures to ensure that financial data is safeguarded and accurate
- Example requirements that affect DBA's:
  - Ensure appropriate database authentication mode is configured
  - Ensure each DBA has own account and no generic accounts used to bypass audit trail of DBA activity
  - Set file system privileges to prevent unauthorized access to database server data files, log files, and backup file
  - Ensure all logins have passwords and not default password
  - Review role memberships and permissions to ensure appropriate access and privileges to databases

FACTA

- Fair and Accurate Credit Transactions Act of 2003 (FACT Act or FACTA)
- Provisions to help reduce identity theft
- Applies to all businesses that maintain consumer information for a business purpose
- Requires merchants to mask most of Credit Card number on store receipts, and not print expiration date

COPPA

- Children's Online Privacy Protection Act (COPPA, 1998)
- Requires parental consent for collection or use of data of website users under age 13

GDPR (EU)

- General Data Protection Regulation (2016)
- **Scope:** Affects all websites processing the personal data of people living in the EU
- **Consent:** Requires consent of users whose info is collected
- **Right to access:** Individuals have the right to access their database
- **Right to be forgotten:** Individuals have the right to have their data erased

Industry Self-Regulation

- US: Payment Card Industry Data Security Standard (PCI DSS)
- Credit card industry standards for protecting credit card info
- Requirements include
  - Encryption of sensitive credit card data (Primary Account Number [PAN], cardholder name, expiration date)
  - No storage at all of CC security authorization code, PIN
  - Minimize cardholder data storage. Develop a data retention and disposal policy. Limit data stored to that which is required for business, legal, and/or regulatory purposes
  - PAN not to be displayed unmasked except for employees with a legitimate business need to see the full PAN

Additional Reading

- Privacy and Human Rights 2003: Overview (privacyinternational.org)
- http://www.ecora.com/ecora/news/whitepaper.asp
  Helpful white papers on regulatory compliance
- https://www.pcisecuritystandards.org
  PCI Security Standards website
- http://it.toolbox.com/blogs/security-compliance/categories
  Security and compliance blogs
- http://www.aclu.org/pizza/
  Pizza video
- https://premium.wpmudev.org/blog/gdpr-how-it-affects-wordpress-site-owners-and-developers/
  GDPR Overview