Contribution to GSR-14: Capitalizing on the Potential of the Digital World

Communications and Information Technology Commission (CITC)

Kingdom of Saudi Arabia

Saudi Arabia embraces principles which protect each individual's right to privacy and prohibit any invasions thereon. The Kingdom has also enacted several laws that establish the regulatory environment related to privacy.

- The telecommunications act and bylaws restrict the disclosure of information that is intercepted during its transmission and restrict ICT service providers from disclosing information regarding their subscribers and from monitoring their communications.
- The anti-cybercrime law defines cybercrimes and prescribes punishments for any person who illegally accesses computers for the purpose of deleting, destroying, altering or redistributing data, who illegally accesses bank or credit information, or who illegally interrupts communications.
- The electronic transactions law regulates exchanges of electronic communications and contracts.
- The credit regulations govern the exchange of information between creditors and borrowers.
- The healthcare practice code requires that health practitioners safeguard the privacy of patients.

The regulatory environment in Saudi Arabia is technology neutral in the sense that it applies to all networks, apps and services related to the storage and transmission of information.

CITC understands that consumers also have a responsibility for protecting their own information and has undertaken an ongoing consumer education program across all media to advise users of safe practices, of their rights and responsibilities, and of their recourse in case of incident.

CITC takes a very active role in all areas of consumer protection, not just privacy and data protection. For example:

- CITC policies allow users to escalate complaints to the Commission within 14 days if not satisfactorily resolved by the service providers.
- Complaints may be registered via the CITC website in Arabic or English.
- CITC maintains a call center for direct communication and follow-up with users.

- CITC actively investigates all registered complaints and maintains statistics on resolution which are available to the public.
- Inappropriate behavior by the service providers may be escalated for judgment as a punishable violation of the telecommunications law.

In addition, the Computer Emergency Readiness Team (CERT-SA) is a functional and very active part of CITC. Besides investigating actual cyber attacks and threats, CERT-SA provides the following services:

- Educational articles on information security as well as specific warnings about viruses and malware on their website.
- An early warning service on threats and possible cyber attacks to registered clients and government agencies.
- A real-time monitoring service for threats and attacks.
- A service which tests clients' systems for vulnerabilities and proposes fixes.