

## searchSecurity.in

### **Radiagate brings information sharing privacy issues to fore**

As the world gets more productive using all-pervasive computers and mobile phones, the amount and range of information generated, stored and shared electronically is increasing dramatically. The sensitivity and importance of such information sharing is also increasing; storage or sharing of personal preference data, credit card details, bank account details and other sensitive information on or over a phone or computer somewhere has become quite routine. Our communication using public or private infrastructure is no exception.

It's no secret that all phone conversations are recorded and retained for a period of at least seven days by service providers or the authorities, in most countries. These measures are deemed necessary to monitor the various communication channels used by terrorists and other potential anti-national elements.

The private data of citizens needs to be made available for legitimate investigative purposes. However, in the process of information sharing, if such data falls into the wrong hands, the consequences could be dangerous.

Theoretically, any one of a total of nine government agencies (including the Intelligence Bureau and Central Board of Direct Taxes) can request for a wiretap, as well as other details such as call logs, text messages, and usage of other services from the telecom company (telco). For information sharing, conversations are recorded and stored in a proprietary format (for example, r4d format) using a communications interception system such as those provided by Verint and similar companies. These details are then uploaded on a server, and later picked up by the concerned agency for investigation.

What happens to the data files after they have been received by the agency is anyone's guess. And, of course, the sensitive information sharing could have taken place among multiple agencies in the first place. In the Radiagate case of a piece of digital information being stolen, it is nearly impossible to track the theft trail, because, unlike a physical theft, the owner remains in possession of the assets even after the theft. Because of the lack of accountability in information sharing, any leak is likely to result in a blame game between various security agencies and the telco.

The solution is to have a mechanism for establishing the custody chain of the information through its lifecycle from the telecom switch to the computer of the investigative officer and beyond. Accountability for ownership is with respect to the original information as well as information shared via copies, wherever they may be.

### **Privacy approaches**

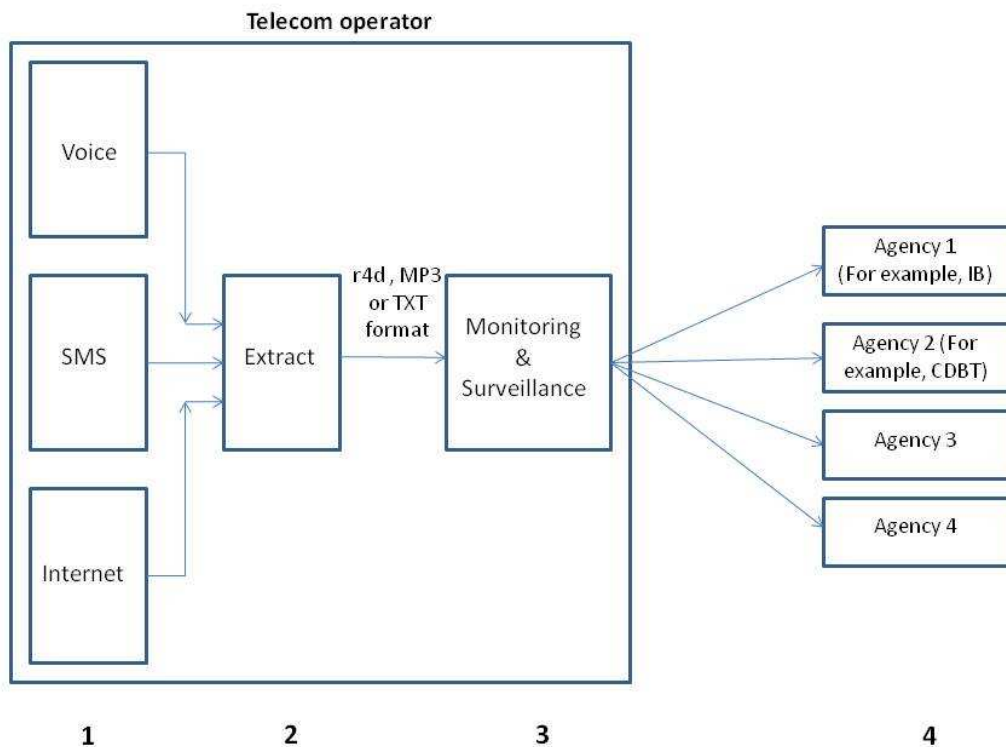
There are various approaches to ensuring the privacy of sensitive information and establishing its chain of custody. One is to create secure "data rooms" within each telco's premises, specifically for information sharing among authorised agencies — carrying data out of this room would be prohibited. The room could actually be a physical one, or it could be "virtualized", and become a virtual data room accessible only from a restricted set of computers or networks. This information sharing approach would increase security, but also would need considerable investment, thus increasing the cost of investigation.

The other approach could be end-to-end encryption of data combined with usage control during information

sharing. Information rights management (IRM) technologies can “protect” information at the source. The protected information and all its copies can then be tracked and controlled (even remotely destroyed) through their lifecycle.

IRM or otherwise, telecom companies and government agencies need to ensure that citizens’ privacy rights are respected, and that usage of any tapped information is carefully controlled. As we stand, it appears that telcos are not using such technology. As a result, it is impossible to trace how information is copied, modified or distributed.

### Chain of custody and data flow process



*Figure 1: Chain of custody and data flow process*

Perusal of Figure1 reveals:

- (1) The telco has different gateways for different data channels (such as the Internet, voice and SMS). Each is typically handled by a different team internally.
- (2) The information is collected from the different gateways to a central collation system; again, this is handled by a separate team.
- (3) Monitoring and surveillance systems are used to process the data. The telco’s team as well as the investigative agency’s team have access.
- (4) The information is made available to the government agencies (the data resides on the servers in the operator’s premises, but access is given to the agencies). Various people within the investigative agency now

gain access to the shared information.

The chain of custody as of now is not clearly established, and information breaches can happen at any level. During information sharing, data is accessible, and available to several people along the chain of custody. In addition, data is in an open format that is easy to clone, and difficult to track.

---

**About the author: Simran Gambhir** is an independent consultant specialising in the realms of bleeding edge technologies. His interest in technology and computer security saw him become a leading developer for media houses such as Fairfax in Australia. He went on to become CTO of News Interactive and Loyalty Pacific. Simran moved to India in 2008, and actively helps VCs perform due diligence on tech companies prior to investment. He is a founding member of null (the Indian open hacker community).

*31 May 2011*

All Rights Reserved, [Copyright 2009 - 2011](#), TechTarget | [Read our Privacy Statement](#)