ENCRYPTICS® {Use Case Scenario}

# Protecting Law Enforcement Sensitive (LES) Data

For the Public Safety Sector

### Goals

- To prevent unintended disclosure of LES data sent via email
- To maintain control of LES data handled outside the agency

### Challenges

- Shrinking budgets and dwindling resources
- Risk of leaks; exposure of LES data to general public

### Requirements

- Scalable, cost-effective solution that requires little to no training
- Support for all network devices (smart phones, tablets, message boards, in-car terminals, etc.)

### Solution

Encryptics for Email™

"To better defend against both external as well as domestic threats and violence, the need for sharing of information between our citizens and state and federal law enforcement agencies has become more acute every day. However, mechanisms to do that in a secured environment are still very vulnerable to cyber threat and attack. There is more of a need than ever to provide our state and local law enforcement agencies with a secure and encrypted environment for sharing information between themselves and the public that they are responsible for protecting.

-Paul Goldenberg, President & CEO
Cardinal Point Strategies

Leading law enforcement agencies are looking to Encryptics® to protect LES data sent via email.

### Situation

Law enforcement executives and officers in all jurisdictions communicate regularly with city leaders, district attorneys, prosecutors, and other public officials. In many cases, email is the most efficient means of communication and often includes LES data, which means dissemination of this data is restricted due to export controls, privacy regulations, court orders, criminal investigations, or matters of national security.

In addition, law enforcement executives and officers are utilizing iPads, iPhones, and Androids for work purposes. This increased mobility enables them to send and receive emails from anywhere—patrol cars, parking lots, coffee shops, etc.—via public networks.

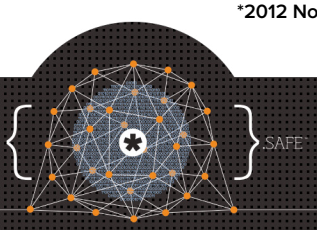
**67%** of people access email via free or unsecured wi-fi connections*

### Security Problem

While convenient, utilizing email to send LES data poses a serious risk to public safety agencies and officials. Because email channels are comprised of countless unsecured networks and servers, information sent via email is vulnerable and can be exposed through unintentional leaks or deliberate theft. Given the sensitive nature of LES data, a leak or theft could result in embarrassing, even disastrous, consequences for the agency or official.

While law enforcement executives and officers may feel that they are sharing LES data only with trusted public officials, a "private" email must essentially cross a cyber-minefield before reaching its destination. Worse yet, if LES data is compromised at any point, there is no way to reclaim or revoke that data. Once sent, copies of LES data can exist all along the email channel on private servers and user devices all over the world. This leaves LES data in the hands of whomever owns (or hacks into) the disk space. Equally troubling, the intended recipient—free to forward, copy, print, or save LES data without the agency's knowledge or permission—can potentially cause as much damage as a hacker.

*2012 Norton Cybercrime Report



Leading law enforcement agencies are looking to Encryptics® to protect LES data sent via email.

## Encryptics for Email Solution

Encryptics for Email is a proactive security solution that will protect law enforcement agencies from the liabilities of email communication. With this solution, law enforcement executives and officials can safely share LES data—contained in messages and attachments—without having to change the way they use email. Supported on mobile as well as desktop devices, this solution provides email security everywhere, even on public networks.

Best of all, Encryptics for Email provides Data Rights Management (DRM), which keeps law enforcement agencies in control of LES data even after it has been sent. This powerful management platform gives senders the ability to prevent Forward, Copy, Print, and Save functions on recipient devices. Senders can also recall sent messages anytime—no matter where they reside.

| Patented | Tested | Validated | Award Winning |
|---|---|---|---|

## Benefits

Law enforcement agencies have a duty to protect LES data from unauthorized dissemination. Agencies that implement Encryptics for Email can be confident that LES data sent via email is protected from the sender's device to the recipient's device and at all points in between. Unauthorized users are kept out and authorized users are kept in line, unable to access, alter, export, or share data unless the agency allows it.

In addition, because Encryptics for Email is a cost-effective solution with a simple onboarding process, agencies won't break budget or sacrifice productivity to get started. With little to no training, users can begin sending secured emails as easily as they send regular emails.

ENCRYPTICS for email

- ✓ True end-to-end data protection
- ✓ Real-time, agency-controlled DRM
- ✓ Cross-platform and mobile support
- ✓ Easy to use, software-based solution

## Summary

Utilizing Encryptics for Email, agencies will assume a heightened level of security that extends beyond the direct jurisdiction of the agency. With a solution that proactively protects against data loss and cyber-attacks, agencies will be able to communicate securely without risk of exposing LES data to unauthorized individuals, malicious groups, and the general public.

### About Encryptics

Encryptics empowers data owners—be that an individual or an agency—by delivering true end-to-end privacy and security solutions. Utilizing a proven, multi-layered encryption and data management platform, these solutions eliminate security risks associated with e-communication, cloud sharing, mobility, and more.

Public and private sector entities across industries rely on Encryptics solutions to protect their critical data from leaks and cyber-attacks.

"You can be more effective if you're confident what you send is going to who you send it to, without worrying about some genius hacking the cloud. Look, the new normal is more access and more engagement with the public we serve. It means most of the time you're out of the office when things go wrong. It means sending and receiving the stuff you need to make a decision, and we better be securing it. We tested Encryptics ,and not only does it secure emails and attachments the moment you press send, you own that content forever. You control who, what, and when they see your data, and that kind of control allows executives to sleep at night.

-Andy Arena, Executive Director
Detroit Crime Commission

visit us on the web
ENCRYPTICS.COM
talk with us
877.503.4781