IT@Intel White Paper
**Intel IT**
IT Best Practices
IT Governance and IT Consumerization
June 2012

# Successful eDiscovery in a Bring-Your-Own-Device Environment

Close collaboration between Intel IT and Intel's legal department strengthens Intel's ability to meet legal obligations as they apply to our bring-your-own-device program.

## Executive Overview

**Intel IT is proactively implementing a bring-your-own-device (BYOD) program that allows employees the flexibility to use personally owned devices such as smartphones and tablets to connect to the corporate network for some IT services. While this presents productivity opportunities to Intel employees, it also poses challenges for Intel IT—including how BYOD affects our legal obligation to fulfill electronic discovery (eDiscovery) requests for data stored on personally owned small form factor (SFF) devices.**

Allowing employees to use their own personal SFF devices to perform corporate job duties presents four primary eDiscovery challenges:

- The company does not own or physically control the devices.
- There are a wide variety of potential data types to consider.
- This data can potentially reside in multiple locations.
- Safeguarding and retrieving the data can be difficult.

To mitigate these challenges, we designed our BYOD program with eDiscovery in mind. We're developing best practices so that our IT eDiscovery team can locate and manage electronically stored information on SFF devices, workstations, or within the enterprise environment. We are also developing applications and recommendations that encourage information to flow through corporate servers. This can help eliminate or reduce the need to harvest data from the employee's device because the same data is available on the corporate servers. Pulling data from the corporate servers also helps us comply with applicable privacy laws. Close collaboration between Intel IT and Intel's legal department strengthens Intel's ability to meet legal obligations as they apply to our BYOD program.

Intel IT's eDiscovery team continues improving processes, procedures, and capabilities in the area of eDiscovery related to personally owned SFF devices—showing that it is possible to move ahead with BYOD initiatives while still addressing potential eDiscovery challenges concerning SFF data.

Steve Watson
Technical Solutions Engineer, eDiscovery, Intel IT

## Contents

## IT@INTEL

The IT@Intel program connects IT professionals around the world with their peers inside our organization – sharing lessons learned, methods and strategies. Our goal is simple: Share Intel IT best practices that create business value and make IT a competitive advantage. Visit us today at www.intel.com/IT or contact your local Intel representative if you'd like to learn more.

## BACKGROUND

**Because many employees are familiar with and increasingly dependent on the ubiquitous computing models provided by consumer-level small form factor (SFF) devices, they want to use their own smartphones and tablets within the enterprise. To meet this growing demand, Intel IT is proactively implementing a bring-your-own-device (BYOD) program that gives employees the flexibility to connect their own devices to the corporate network for some IT services. While this presents productivity opportunities to Intel employees, it also poses challenges for Intel IT—including how BYOD could affect our ability to fulfill electronic discovery (eDiscovery) requests for data stored on those personally owned SFF devices.**

Discovery—pretrial procedures involving the exchange of information between parties involved in a legal proceeding—has significantly changed in the last 10 years. As more companies use electronic means to store and share data, electronic documents and eDiscovery have taken an increasingly prominent role in litigation.

In late 2006, the U.S. Federal Rules of Civil Procedure was updated with specific rules and definitions relating to the discovery of electronically stored information (ESI). The new rules defined that ESI would be considered "documents," removing any remaining ambiguity that ESI is subject to the exchange of information that occurs in civil litigation. This evolution brought into focus the many forms of ESI that companies around the world rely on to do business. Email, backup tapes, instant messaging, and potentially even data found on SFF devices, could all be identified for discovery requests.

Like many large corporations, Intel is regularly involved in multiple civil court cases relating to intellectual property and other corporate legal matters. Therefore, our legal teams are proactive in the area of eDiscovery, with teams and processes in place to respond to changes in the legal and technology landscapes. We continue to expand and adjust our eDiscovery processes as technology advances. Without a thorough review of eDiscovery obligations, including those in the area of personally owned SFF devices, an Intel legal team's efficiency, credibility, and ability to meet its legal obligations in the courtroom could be in jeopardy.

## ADDRESSING THE PRIMARY eDISCOVERY CHALLENGES ASSOCIATED WITH PERSONALLY OWNED SFF DEVICES

**In our experience, any data in the enterprise may be identified for a legal matter—ranging from sensitive financial and intellectual property data to the seemingly benign, casual instant message. Intel IT's eDiscovery team needs to be able to locate and access ESI wherever it exists in the enterprise, whether that data is on corporate backup tapes, laptops, desktop PCs, or on personally owned tablets and smartphones.**

Any time employees bring their own devices to the workplace there is the potential that corporate data may end up on those devices. This is especially true at Intel as we actively implement a BYOD SFF initiative, called Handheld Services. Our BYOD program allows employees who sign a service agreement to use their personally owned devices at work. At the time of this writing, Intel IT supports 33,000 handheld devices—60 percent of which are the personal property of employees.

Allowing the use of personally owned SFF devices to perform corporate job duties presents four primary challenges for Intel IT and Intel's eDiscovery teams.

- The company does not own or physically control the devices.
- A wide variety of potential data types need to be considered.
- The data can potentially reside in multiple locations.
- Safeguarding and retrieving the data can be difficult.

Intel IT's eDiscovery team continues developing processes, procedures, and capabilities in the area of eDiscovery as it relates to personally owned SFF devices—showing that it is possible to move ahead with BYOD initiatives without hampering our ability to meet legal obligations. Table 1 summarizes our approach to some of our most common SFF-related eDiscovery challenges.

## Maintaining Access to and Control of the Data and the Device

An IT department can help attorneys understand how the SFF computing infrastructure affects eDiscovery—where SFF data is located, what data can be retrieved, and how data can be retrieved. By definition, personally owned SFF devices lie outside of the routine access and physical control of the company. Employees manage their own devices, and they decide if they bring them to work. Employees also control what data their devices access and store. For example, although Intel IT offers email, contact, and calendar services to personally owned SFF devices registered with our Handheld Services program, we cannot predict which, if any, of these services employees actually use and when they use them.

This situation raises the question of how Intel can address a request for data when that data might reside on an employee's SFF device. Because personally owned SFF devices are not corporate property, Intel IT's eDiscovery team cannot simply seize a device, even when we have the legal obligation to collect the data it contains—we need the employee's consent and cooperation.

Intel IT has addressed the data retrieval issues by requiring employees who participate in the Handheld Services program to sign a service agreement. This service agreement seeks to balance employee privacy rights while attempting to address corporate data security and eDiscovery concerns.

## Managing Multiple Categories of Data

Data residing on a personally owned SFF device can be categorized in multiple ways, each of which could raise eDiscovery issues. Three ways of categorizing the data as a means of exploring the data types are as follows:

- Corporate data and non-corporate data, which includes personal information
- Device-created data, application-created data, and user-created data
- Retrievable data and irretrievable data

The following subsections discuss how each of these methods of data categorization can affect eDiscovery processes, and provide examples of how Intel IT handles data-related challenges.

Table 1. Summary of Small Form Factor eDiscovery Challenges

| Challenge | Potential Problem(s) | Intel IT's Approach |
|---|---|---|
| Access to and Control of Data and Device | Device and data outside direct corporate control | Use a service agreement, signed by the employee, to specify how electronic discovery (eDiscovery) requests will be handled. |
| Multiple Categories of Data | Corporate and non-corporate information may be intermingled | Collect only the most pertinent data by using targeted collection techniques and provide applications that use corporate servers to interact with the environment. |
| | Some data may be irretrievable | Look for the same data in a more readily accessible location on the enterprise network, use multiple mobile forensic applications, or resort to lower-tech solutions when necessary. |
| Data Location | Corporate data that may exist only on the small form factor (SFF) device | For employees that might be identified in a legal matter, encourage them to synchronize their SFF devices to an alternate location on the network. |
| Data Retrieval Process | Properly managing data retrieval | Establish a well-defined chain of custody and adhere to proper data handling and established forensic procedures to preserve data integrity. |

Table 2. Data Definitions

| Term | Definition |
|---|---|
| Corporate Data | Data associated with the enterprise, such as corporate email messages, documents, and text messages |
| Non-corporate Data (includes personal information) | Non-corporate data includes documents that an individual creates or stores on the device, along with personal information such as email contacts and photos |

## CORPORATE AND NON-CORPORATE DATA

Personally owned SFF devices used in a corporate environment will likely contain a mix of corporate and non-corporate data as defined in Table 2.

Ideally, eDiscovery teams would be able to ignore everything except corporate data, but the current underlying architecture of SFF devices and operating systems does not support the native separation of corporate and other data. For example, all email—both personal and corporate—may be stored in the same email database on the device. Also, eDiscovery teams must be aware of the varying requirements for defining and handling personal information in different regions and countries.

To collect as little non-corporate data as possible, the Intel IT eDiscovery team uses the following guidelines:

- Clarifies and pinpoints the request for data from the legal team, whenever possible. For example, if the legal team requests only call history, we use a tool and process that collects only that data from the device, which minimizes the inadvertent collection of personal information.
- Encourages employees to save corporate data to the corporate network instead of on the SFF device. This helps minimize the corporate data that may exist solely on the device and simplifies data collection. During the eDiscovery process, our IT eDiscovery teams make an effort to identify corporate data on other sources, such as corporate servers, whenever possible.
- Works with the legal team to meet eDiscovery obligations in full compliance with applicable and governing privacy and data protection laws and agreements.
- Provides guidance, through the Appropriate Use Policy, about acceptable use policies. For example, Intel's service agreement specifies that an employee must follow Intel's email, Internet, and computer-use guidelines when using a personally owned SFF device that is connected to an Intel network or logged into an Intel account.

## DEVICE-CREATED, APPLICATION-CREATED, AND USER-CREATED DATA

How the data was created is another way to categorize data on a SFF device. Examples of device-created data might include when the device was turned on or off, and time and date of the last synchronization with desktop software. Examples of application-created data include the browser cache that is created when a user browses the Internet using the device, and application statistics of how often a particular game is played or what the high scores were. Examples of user-created data include notes typed by the user, contact lists, personal diaries, documents, and calendar entries.

For eDiscovery matters, however, device-created and application-created data is usually not relevant to a legal matter. Most eDiscovery requests in civil litigation focus on user-created data.

## RETRIEVABLE AND IRRETRIEVABLE DATA

eDiscovery applications focused on user PCs or corporate servers historically have not been able to collect data from mobile or SFF devices. This has led to a proliferation of specialized mobile device forensic applications, with new solution providers appearing every year. A major challenge in SFF data retrieval is that SFF manufacturers do not reveal how data is actually stored on the devices they make. Therefore, companies that create mobile device forensics applications must reverse engineer how to harvest SFF data, a process that is not always successful. And, because eDiscovery forensics is a highly competitive market, solution providers do not share their data harvesting methodologies.

Therefore, it is not uncommon for the results from two different mobile forensic applications that are attempting to harvest the same data to have subtle differences, and results can differ between device makes and models. For example, one forensic tool may be able to successfully gather all business contact info, except the business fax number; another may be able to pull only names and zip codes from the same data.

Following industry best practices, Intel IT's eDiscovery team may use multiple forensic tools on an SFF device to to collect data with user consent and in compliance with our privacy and data security policies. If the data is irretrievable through data harvesting, we may use a lower-tech solution, such as taking a photograph of the data on the device's screen. Additionally, understanding what data types the legal team is looking for may help us find the requested data in other corporate network locations.

## Understanding Where Data Might Reside

Knowing where data can reside is a key to successfully navigating an eDiscovery request. There are four primary locations where SFF data may reside: the corporate network and cloud, the telecommunications carrier, the SFF device itself, or an employee's corporate PC. The types of data typically found in each of these locations are summarized in Table 3.

In our experience, if ESI is on the corporate network, we may be able to meet eDiscovery requirements without needing access to the employee's SFF device. This is our preferred solution to data retrieval. Similarly, if employees dock their personally owned SFF devices, an automatic backup or synchronization may occur, depending on the device type and configuration. Often, the data stored in the backup is equal to or of better quality than data retrieved from the SFF device itself.

Table 3. Typical Data Locations and Types of Data on Personally Owned Small Form Factor Devices

| Typical Data Location | Typical Data Types |
|---|---|
| Corporate Network and Cloud | ▪ Corporate email, calendar, and contacts<br>▪ User-created data that is saved<br>▪ User connection or session information saved in log files of network connection or application session<br>▪ Device information, if a mobile device management solution manages corporate connectivity |
| Telecommunications Carrier | ▪ Call logs beyond the history of the phone<br>▪ Short Message Service (SMS) and Multimedia Messaging Service (MMS) messages beyond the history of the phone<br>▪ Global Positioning System (GPS) or tower location tracked by the carrier<br>▪ Voicemails<br>▪ Usage information |
| Small Form Factor (SFF) Device | ▪ Call logs<br>▪ Network logs<br>▪ SMS and MMS messages<br>▪ GPS or tower location information<br>▪ User-created and non-user-created music, photos, movies, and videos<br>▪ Web browser history, cache, and bookmarks<br>▪ Text notes<br>▪ Email, calendar, and contact information<br>▪ User-created documents<br>▪ User-synchronized documents<br>▪ SFF synchronization and backup log |
| Employee's Corporate PC | ▪ User-created data potentially synchronized from the SFF device to the PC<br>▪ Photos or music synchronized to the PC<br>▪ Backup of SFF device<br>▪ Source or duplication of email, calendar, and personal or corporate contacts that may exist on the SFF device<br>▪ Source or duplication of user-created data saved to the cloud or enterprise network<br>▪ SFF synchronization or backup log |

Certain data is impossible to retrieve. For example, SFF devices do not store unlimited call history or text message data; the browser history and cache are limited by a finite amount of memory and are flushed by the device after a certain data size is met; and some devices store synchronization information in a readily accessible location, while others do not. Although more complete data may in theory be available from the telecommunication carrier, carriers are typically unwilling to provide data for eDiscovery requests that don't come from law enforcement or a court with the appropriate jurisdiction and documentation.

Understanding where data might be located and whether it can be harvested helps our IT eDiscovery team avoid committing to providing data that may actually be unavailable.

## Managing the Data Retrieval Process

Intel's eDiscovery teams work to maintain a good chain of custody process, which includes chronological documentation of the access, collection, transfer, and storage of data. Proper data handling and established forensic procedures are required to preserve data integrity.

When performing eDiscovery on SFF devices, network isolation is vitally important. SFF devices may have multiple communication channels, such as a mobile network, Wi-Fi*, and Bluetooth*; therefore, it may be necessary that the device be unable to contact a network from the time at which IT takes possession of the device until after the data is collected. If an SFF device is allowed to communicate with a network, changes may occur to the data on the device. Potential changes could include remote wiping of the device and synchronization of data—including the addition of new information or deletion of old information. Network isolation can be achieved through the use of Faraday cages, boxes, or bags that block communication signals, or may be achieved by disabling network services to the device.

Within our well-established process to maintain chain of custody, Intel attorneys work closely with IT to choose the right tools to adequately and appropriately respond to eDiscovery requests. We provide our SFF data preservation teams with the appropriate training and certifications, so that the preservation is legally defensible. Our IT eDiscovery team has an established protocol, shared with the Intel legal team, concerning how network isolation will be maintained during custody and collection.

### FORENSIC ANALYSIS OF THE SFF DEVICE

When the IT eDiscovery team has physical access to the SFF device, traditional forensic collection and analysis of the device can be completed. We inform the Intel legal team that data harvested from the device may be in a different file format, or presented in a different form, than the attorneys are used to seeing. For example, SFF devices make frequent use of .plist files and SQLite databases to store information, so what may look like a calendar entry or contact on the device could be exported as a table. Some mobile device forensics applications seek to normalize the data view to ensure that emails look like emails or contacts look like contacts when the final data is extracted and provided to the attorneys.

If data can be retrieved from a preferred data source such as corporate servers, the IT eDiscovery team may not have to harvest data from the SFF device at all. However, if data is harvested from the SFF device, the forensic collection should retrieve, at a minimum, all readily retrievable data from the device. At the direction of the legal team, analysis could exclude non-relevant data types or focus on a particular data category for retrieval. Analysis may also include analyzing data by chronology, off-device data locations, data type, or keyword searches in the harvested data.

### EXPORT AND PRESERVATION FROM THE CLOUD AND ENTERPRISE APPLICATIONS

If most corporate data on the device is configured to synchronize with or be automatically saved to the corporate network, the SFF device will store minimal or duplicate corporate data. In this situation, the data on the device is often cached information or incomplete compared to the data stored on the corporate servers.

For example, if the SFF device's email configuration saves email changes back to the user's corporate mailbox instead of to the SFF device, the corporate server becomes the best source of collection.

As more applications and enterprise network locations become accessible to SFF devices, we have found that it is worthwhile to educate employees about the importance of saving data to the corporate network. We encourage our IT solution developers to design applications and corporate networks with the goal of saving minimal corporate data to any SFF device—allowing us to enable BYOD capability and mitigate the risk of where the data resides.

# BEST PRACTICES FOR eDISCOVERY ON SFF DEVICES

**Based on our experience with Intel's BYOD program, we have identified best practices for managing eDiscovery on personally owned SFF devices. Because eDiscovery involves more than just IT or legal teams, different best practices are important for different participants in the eDiscovery process.**

The following subsections list and discuss the best practices we have developed for our IT department, IT eDiscovery teams, and forensic investigators. We also discuss some areas where we believe SFF device manufacturers, mobile forensic application solution providers, and mobile device management (MDM) suppliers could provide enhancements to make eDiscovery on personally owned SFF devices easier and more productive.

## IT Department

The IT department, especially in the area of infrastructure design, can significantly aid eDiscovery efforts. Before deploying our BYOD program, we gave serious thought to creating an infrastructure that could allow employees choice in using personal SFF devices while maintaining our ability to perform excellent eDiscovery:

- Provide early input on requirements for BYOD enterprise deployment. For example, for corporate email, users can interact with email on an SFF device, but all email traffic—send, receive, and open mail operations—goes through corporate servers. In this way, we avoid having to harvest data from the employee's device because the same data is available on the corporate servers.
- Investigate MDM solutions that are coming to market. MDM solutions may help identify where data is saved and limit what can be saved to a SFF device.
- Identify the enterprise locations where the data can be preserved.

## IT eDiscovery Teams and Forensic Investigators

IT eDiscovery teams and forensic investigators can maximize the value of a well-designed BYOD infrastructure by adopting these guidelines:

- Follow industry best practices for SFF device acquisition, handling, and chain of custody procedures.
- Obtain training on existing and emerging SFF forensics capabilities.
- Work with privacy, Human Resources, and litigation teams to clearly define the processes regarding corporate and personal data distinction, collection, and disposal.
- Work with the legal team requesting data to explicitly understand the data types needed for collection.

## Industry Players

The growth of the importance of eDiscovery has led to a proliferation of experts and eDiscovery applications and solutions providers to help companies comply with legal requirements. Although current mobile forensic applications aid in eDiscovery on personally owned SFF devices, there are several areas where maturation in the marketplace—especially for the device manufacturers—could improve eDiscovery capabilities:

- Native data separation or containerization. SFF device architecture does not currently support the separation of corporate and personal data by means of containerization or some other distinction. Today this would require a third-party MDM management application to enable it on the device, which would mean significant changes to the architecture of SFF operating systems.
- Remote access to data. As SFF devices are network-connected devices, application vendors should seek to create technologies that enable remote, over-the-wire collection of available logical data. This would allow for data collection without physical possession of the device.
- Open source data harvesting methodologies. Few open source applications exist for the collection of SFF device data. There is a pressing need for open source collection capabilities, data parsers, and normalization of .plists and SQlite database information.

## CONCLUSION

**With our BYOD program, Intel IT is taking a proactive approach to enabling personal devices in the enterprise in a secure manner, achieving the benefits of increased security, employee productivity, flexibility, and satisfaction at low cost to Intel. But along with these benefits come challenges. One of those challenges is how to perform eDiscovery on personally owned SFF devices.**

By their very nature, personally owned SFF devices are outside of the physical control of the corporation, and are likely to contain both personal and corporate data. Because employees' SFF devices may not always be synchronized with a corporate PC or the enterprise network, questions arise about where data resides, and the existing SFF device architecture does not always optimally support data preservation.

To address these issues, we have developed best practices for managing eDiscovery on personally owned SFF devices and designed a BYOD infrastructure that supports successful eDiscovery. Our corporate IT department collaborates closely with Intel IT's eDiscovery teams and with Intel's legal department so that we can find ESI wherever it exists in the enterprise—on corporate backup tapes, laptops, desktop PCs, or on employees' personal tablets and smartphones.

By implementing these best practices, we can move ahead with BYOD initiatives that enhance employee productivity and job satisfaction, while effectively addressing potential eDiscovery challenges that arise related to SFF data.

## ACRONYMS

| | |
|---|---|
| BYOD | bring-your-own-device |
| eDiscovery | electronic discovery |
| ESI | electronically stored information |
| GPS | global positioning system |
| MDM | mobile device management |
| MMS | Multimedia Messaging Service |
| SFF | small form factor |
| SMS | Short Message Service |

**For more information on Intel IT best practices, visit www.intel.com/it.**

This paper does not purport to state the law, offer a legal opinion, or reflect variants in the law. It mentions these concepts in general solely to reflect Intel IT's role in addressing eDiscovery requests.

This paper is for informational purposes only. THIS DOCUMENT IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE. Intel disclaims all liability, including liability for infringement of any patent, copyright, or other intellectual property rights, relating to use of information in this specification. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted herein.

Printed in USA ♲ Please Recycle 0612/ERAI/KC/PDF 327404-001US