IT@Intel Executive Summary
Intel IT
IT Best Practices
IT Governance and IT Consumerization
June 2012

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

Best Practices for eDiscovery on Personally Owned Small Form Factor Devices:

- Can address challenges associated with device access and control, data types and location, and data retrieval processes
- Support BYOD initiatives that enhance employee productivity and job satisfaction, while enabling an Intel legal team's ability to meet its legal obligations in the courtroom

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.

Addressing The Primary eDiscovery Challenges Associated With Personally Owned SFF Devices

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.** 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. 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.
- **There are a wide variety of potential data types to consider.** Data residing on a personally owned SFF device can be categorized in multiple ways, including corporate and non-corporate; device-created data, application-created data, and user-created data; and retrievable data and irretrievable data. Each of these methods of data categorization can affect eDiscovery processes.
- **Data can potentially reside in multiple locations.** 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.
- **Safeguarding and retrieving the data can be difficult.** Proper data handling and established forensic procedures are required to preserve data integrity. Issues to consider are chain of custody procedures, network isolation, and encouraging employees to synchronize their devices with the corporate network.

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.

In addition to the best practices we have developed for Intel IT and IT eDiscovery teams and forensic investigators, we have also identified several areas where maturation in the marketplace—especially for the device manufacturers—could improve eDiscovery capabilities. Examples of these improvements include the following:

- Native data separation or containerization
- Remote access to data
- Open source data harvesting methodologies

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.

You can find a full discussion of eDiscovery and BYOD at Intel at "Successful eDiscovery in a Bring-Your-Own-Device Environment."

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 proprietary 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.