SCHEDULE A

1. Deleted, slack, fragmented, or other data only accessible by forensics.

2. Random access memory (RAM), temporary files, or other ephemeral data that are difficult to preserve without disabling the operating system.

3. On-line access data such as temporary internet files, history, cache, cookies, and the like.

4. Data in metadata fields that are frequently updated automatically, such as last-opened dates.

5. Back-up data that are substantially duplicative of data that are more accessible elsewhere.

6. Voice messages.

7. Instant messages that are not ordinarily printed or maintained in a server dedicated to instant messaging.

8. Electronic mail or pin-to-pin messages sent to or from mobile devices (e.g., iPhone and Blackberry devices), provided that a copy of such mail is routinely saved elsewhere.

9. Other electronic data stored on a mobile device, such as calendar or contact data or notes, provided that a copy of such information is routinely saved elsewhere.

10. Logs of calls made from mobile devices.

11. Server, system or network logs.

12. Electronic data temporarily stored by laboratory equipment or attached electronic

equipment, provided that such data is not ordinarily preserved as part of a laboratory report.

13. Data remaining from systems no longer in use that is unintelligible on the systems in use.