LIMITLESS SURVEILLANCE AT THE FDA: PROTECTING THE RIGHTS OF FEDERAL WHISTLEBLOWERS

JOINT STAFF REPORT

Prepared for

Representative Darrell E. Issa, Chairman
Committee on Oversight and Government Reform
United States House of Representatives
&
Senator Charles E. Grassley, Ranking Member
Committee on the Judiciary
United States Senate

113th Congress
February 26, 2014

I. Table of Contents

II. Table of Names

Food and Drug Administration

Jeffrey Shuren
Director, Center for Devices and Radiological Health

Jeffrey Shuren is the Director for the Center for Devices and Radiological Health. He oversees the Center's operations and strategic direction. Dr. Shuren, along with several other FDA officials, ordered the initial computer monitoring and was a later proponent of its expansion.

Ruth McKee
Associate Director for Management and Executive Officer, Center for Devices and Radiological Health

Ruth McKee is the Associate Director for Management and Executive Officer for the Center for Devices and Radiological Health. McKee reports directly to Dr. Shuren, who tasked her to lead the charge to determine what steps the FDA needed to take after it learned of the potential leak. McKee also ordered the monitoring and determined the initial monitoring search terms given to the Office of Information Management.

Mary Pastel
Deputy Director for Radiological Health for In Vitro Diagnostics, Center for Devices and Radiological Health

Mary Pastel is the Deputy Director for Radiological Health for *In Vitro* Diagnostics with the Center for Devices and Radiological Health. Ruth McKee instructed Pastel to review encrypted flash drives containing surveillance of information on scientists' computers.

Lori Davis
Chief Information Officer

Lori Davis was the Chief Information Officer for the FDA. Prior to being named the Chief Information Officer in January 2009, she served as the Deputy Chief Information Officer. She worked with Ruth McKee to set up computer monitoring of Dr. Robert Smith, and was asked to search through e-mails of FDA employees to determine the source of the information leak.

Joe Albaugh
Chief Information Security Officer

Joe Albaugh was the Chief Information Security Officer for the FDA until March 2011. Lori Davis approached Albaugh to set up the computer monitoring for Dr. Robert Smith.

Robert Smith
Medical Officer, Center for Devices and Radiological Health

Robert Smith was a Medical Officer for the Center for Devices and Radiological Health. He was the first employee at the FDA to experience computer monitoring. Based on information gathered from Dr. Smith's computer, officials at the FDA later expanded this monitoring to include additional FDA scientists. His contract was not renewed after his contacts with Congress, the Office of Special Counsel, and his personal attorney were captured through the FDA's monitoring program.

Les Weinstein
Ombudsman, Center for Devices and Radiological Health

Les Weinstein was the Ombudsman in the Office of the Center Director for the Center for Devices and Radiological Health. Weinstein asked the U.S. Department of Health and Human Services Office of Inspector General to investigate the disclosure of confidential information to the press.

Chickasaw Nation Industries Information Technology, LLC

Christopher Newsom
Contract Forensic Engineer, Incident Response Team

Christopher Newsom is a Forensic Engineer with Chickasaw Nation Industries Information Technology. Newsom conducted the computer monitoring of FDA employees. After the FDA first set up this monitoring for Dr. Robert Smith, Newsom prepared an interim report to summarize the status of the monitoring.

Joseph Hoofnagle
Contract Investigator, Incident Response Team

Joseph Hoofnagle is a Contract Investigator with Chickasaw Nation Industries Information Technology. Hoofnagle installed Spector 360 software on the monitored employees' computers. He worked with Newsom to conduct computer monitoring of FDA employees, and assisted Newsom in writing an interim report to summarize the status of the monitoring.

communications, communications with Congress, and communications with the OSC. The FDA intercepted communications with congressional staffers and draft versions of whistleblower complaints complete with editing notes in the margins.[8] The agency also took electronic snapshots of the computer desktops of the FDA employees and reviewed documents and files they saved on the hard drives of their government computers as well as personal thumb drives attached to their computers.[9] FDA even reconstructed files that had been deleted from personal thumb drives prior to the device being used on an FDA computer.

The contractors conducting the investigation prepared an interim report to update FDA officials.[10] This report, which was sent to Deputy Chief Information Officer Lori Davis on June 3, 2010, attempted—yet could not definitively support—a link to Dr. Smith with the release of 510(k) information to non-FDA employees.[11] The report described information found on Dr. Smith's computer, including e-mails with journalists, Congress, and the Project on Government Oversight.[12] The report also stated that Dr. Smith "ghostwrote" reports for his subordinates and supplied internal CDRH documents to external sources.[13] After receiving this report, the FDA expanded the computer monitoring to include three additional CDRH scientists[14] and declined to renew Dr. Smith's contract.[15]

FDA officials also contacted the Department of Health and Human Services (HHS) Office of Inspector General (OIG) on numerous occasions to request an investigation into the disclosures.[16] The OIG declined these requests, noting that contacts with the media and Congress were lawful, and no evidence of criminal conduct existed.[17] Despite the OIG's repeated refusal to investigate, the FDA continued to monitor Dr. Smith and his colleagues in the hope of finding enough evidence to convince the OIG to take action.[18] However, the FDA failed to take direct administrative or management action on its own to address the concerns directly.

---

[8] Ellen Nakashima and Lisa Rein, *FDA staffers sue agency over surveillance of personal e-mail,* WASH. POST, Jan. 29, 2012.
[9] *Id.*
[10] Memorandum from Joseph Hoofnagle, Incident Response & Forensic Lead & Christopher Newsom, Incident Response & Forensic Investigator, *Interim Report of Investigation – Robert C. Smith* (June 3, 2010) [hereinafter Interim Report].
[11] *Id.*
[12] *Id.*
[13] *Id.*
[14] McKee Tr. at 16.
[15] *Id.* at 33.
[16] Letter from Jeffrey Shuren, Dir., Ctr. for Devices & Radiological Health, FDA, to Daniel R. Levinson, Inspector Gen., Dep't of Health & Human Servs. (Feb. 23, 2011) [hereinafter Shuren Letter, Feb. 23, 2011]; Letter from Les Weinstein, Ombudsman, Center for Devices & Radiological Health (CDRH), FDA, to Leslie W. Hollie, Supervisory Special Agent, Office of Investigations, Office of Inspector Gen., U.S. Dep't of Health & Human Servs. (HHS) (Mar. 23, 2009); E-mail from Les Weinstein, Ombudsman, CDRH, FDA, to Leslie W. Hollie, Supervisory Special Agent, Office of Investigations, Office of Inspector Gen., HHS (Oct. 23, 2009, 6:06 p.m.) [hereinafter Weinstein E-mail].
[17] Letter from Scott A. Vantrease, Asst. Special Agent in Charge, Special Investigations Branch, Office of the Inspector Gen., HHS, to Mark McCormack, Special Agent in Charge, Office of Criminal Investigations, Office of Internal Affairs, FDA (May 18, 2010) [hereinafter Vantrease Letter].
[18] H. Comm. on Oversight & Gov't Reform, Transcribed Interview of Jeffrey Shuren, at 20-21 (Nov. 30, 2012) [hereinafter Shuren Tr.].

III. Executive Summary

In January 2009, several national news outlets, including the *New York Times*, *Associated Press*, and the *Wall Street Journal*, reported that U.S. Food and Drug Administration (FDA) scientists had lodged complaints that the agency was approving unsafe and risky medical devices.[1] In March 2010, the *New York Times* published a follow-up article reporting allegations by FDA scientists that the FDA ignored radiation warnings when approving certain medical devices.[2]

Specifically, Dr. Robert Smith and four other employees of the FDA's Center for Devices and Radiological Health (CDRH) expressed concern about FDA-approved medical devices. Dr. Smith believed FDA managers ignored warnings from scientists regarding potential health hazards related to radiation exposure. Dr. Smith and the other CDRH employees also expressed their concerns to Congress and the 2009 White House Transition Team.[3] Additionally, Dr. Smith and his colleagues reported allegations of retaliation to Congress and the U.S. Office of Special Counsel (OSC).[4]

Upon learning CDRH scientists publicly disclosed information about pending device applications, known as 510(k) applications, CDRH management initiated an electronic surveillance program of unprecedented scope. To determine which scientists were disclosing information and what specific information they were disclosing, the CDRH engaged two contractors working on the FDA's information technology security systems in April 2010 to begin monitoring Dr. Smith.[5] Approximately one month later, the monitoring expanded to another CDRH scientist.[6] Using a software monitoring program called Spector 360, which took screenshots of FDA employees' computers every five seconds,[7] FDA officials were able to obtain sensitive information and protected communications, including attorney-client

[1] Gardiner Harris, *In F.D.A. Files, Claims of Rush to Approve Devices*, N.Y. TIMES, Jan. 13, 2009, *available at* http://www.nytimes.com/2009/01/13/health/policy/13fda.html?_r=0 (last visited Feb. 21, 2014) [hereinafter *Rush to Approve Devices*]; Ricardo Alonso-Zaldivar, *FDA Scientists Complain to Obama of 'Corruption,'* ASSOC. PRESS, Jan. 8, 2009 [hereinafter *Scientists Complain to Obama*]; Alicia Mundy & Jared Favole, *FDA Scientists Ask Obama to Restructure Drug Agency*, WALL ST. J., Jan. 8, 2009, *available at* http://online.wsj.com/news/articles/SB123142562104564381 (last visited Feb. 21, 2014).

[2] Gardiner Harris, *Scientists Say F.D.A. Ignored Radiation Warnings*, N.Y. TIMES, Mar. 28, 2010, *available at* http://www.nytimes.com/2010/03/29/health/policy/29fda.html?pagewanted=all (last visited Feb. 21, 2014) [hereinafter *F.D.A. Ignored Radiation Warnings*].

[3] *Scientists Complain to Obama*, *supra* note 1.

[4] Letter from Lindsey M. Williams, Dir. of Advocacy & Dev., Nat'l Whistleblowers Ctr., to Sen. Chuck Grassley, Ranking Member, Senate Judiciary Comm., Chairman Darrell Issa, H. Comm. on Oversight & Gov't Reform, & Special Counsel Carolyn Lerner, U.S. Office of Special Counsel (Sept. 17, 2012) [hereinafter NWC Letter]; Letter from CDRH Scientists, Office of Device Evaluation, Food & Drug Admin. (FDA), to Rep. John Dingell, U.S. House of Representatives (Oct. 14, 2008) [hereinafter CDRH Letter].

[5] H. Comm. on Oversight & Gov't Reform, Transcribed Interview of Ruth McKee, at 7-9 (Nov. 13, 2012) [hereinafter McKee Tr.].

[6] *See* Letter from Jeanne Ireland, Ass't Comm'r for Legis., FDA, to Hon. Darrell E. Issa, Chairman, H. Comm. on Oversight and Gov't Reform (July 13, 2012) [hereinafter Ireland Letter].

[7] H. Comm. on Oversight & Gov't Reform, Transcribed Interview of Christopher Newsom, at 10-11 (Oct. 2, 2012) [hereinafter Newsom Tr.].

FDA officials eventually forwarded information gathered from the computer monitoring program to the OIG.[19] The OIG contacted the Criminal Division of the Department of Justice to determine whether the evidence collected by the FDA against Dr. Smith and his colleagues supported a criminal referral.[20] In November 2010, by letter, the Criminal Division formally declined to take up the matter.[21]

FDA's overly-invasive monitoring program came to light in January 2012, when Dr. Smith and several of his colleagues filed a lawsuit in U.S. District Court in Washington, D.C. The suit alleged that information gathered during the monitoring was used to harass or dismiss at least six current and former FDA employees. House Committee on Oversight and Government Reform Chairman Darrell Issa and Senate Committee on the Judiciary Ranking Member Charles Grassley (the Committees) subsequently launched a joint investigation into the monitoring program.

In May 2012, documents associated with the monitoring were posted on a public internet site. Included in these materials were confidential and proprietary FDA documents, as well as confidential communications between FDA employees and Congress, the OSC, and personal attorneys.[22]

Witnesses who contacted the Committees voiced concerns about the intrusive nature of the surveillance, and the irresponsibility in posting the fruits of the surveillance on the Internet for anyone to see. They believed that the FDA conducted surveillance for the sole purpose of retaliating against the scientists for raising concerns about the medical device review process.

The Committees conducted seven transcribed interviews with current and former FDA employees and contractors and reviewed approximately 70,000 documents. The pace of the Committees' investigation was slowed by FDA's unwillingness to cooperate. The FDA repeatedly cited the ongoing litigation with Dr. Smith and his colleagues as an excuse to withhold documents and information.

Documents and information obtained by the Committees show the FDA conducted this monitoring program without regard for employees' rights to communicate with Congress, the OSC, or their personal attorneys. The Committees' investigation also found that data collected could be used to justify adverse personnel actions against agency whistleblowers. Absent a lawful purpose, an agency should not conduct such invasive monitoring of employees' computer activity. The FDA failed not only to manage the monitoring program responsibly, but also to consider any potential legal limits on its authority to conduct surveillance of its employees. The Committees' investigation has shown that agencies need clearer policies addressing appropriate monitoring practices to ensure that agency officials do not order or conduct surveillance beyond their legal authority or in order to retaliate against whistleblowers, especially in such a way that

---

[19] Letter from Jeffrey Shuren, Dir., Ctr. for Devices & Radiological Health, FDA, to Hon. Daniel Levinson, Inspector Gen., Dep't of Health & Human Servs. (June 28, 2010) [hereinafter Shuren Letter, June 28, 2010].
[20] Shuren Tr. at 67-68.
[21] Letter from Jack Smith, Chief, Public Integrity Section, Dep't of Justice, to David Mehring, Special Agent, Office of the Inspector Gen., Dep't of Health & Human Servs. (Nov. 3, 2010) [hereinafter DOJ Letter].
[22] *Id.*

chills whistleblower communications with Congress, the OSC, and Inspectors General.[23] Congress has a strong interest in keeping such lines of communication open, primarily as a deterrent to waste, fraud, and abuse in Executive Branch departments and agencies.

Whistleblower disclosures are protected by law, even if they are ultimately unsubstantiated, so long as the disclosure was made in good faith. Accordingly, the analysis of the issues examined in this report is not dependent on the merits of the underlying claims that whistleblowers made about the safety of certain medical devices. Thus, this report does not examine the merits of those underlying claims and takes no position on whether the devices in question posed a risk to public health.

[23] The Whistleblower Protection Act provides protections for whistleblowers against personnel actions taken because of a protected disclosure made by a covered employee. The Act provides that "any disclosure of information" made by a covered employee who "reasonably believes" evidences "a violation of any law, rule, or regulation" or evidences "gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety" so long as the disclosure is not prohibited by law nor required to be kept secret by Executive Order. *See* 5 U.S.C. § 2302(b)(8)(A); Cong. Research Serv., Whistleblower Protection Act: An Overview, at 3 (Mar. 12, 2007), *available at* http://www.fas.org/sgp/crs/natsec/RL33918.pdf (last visited Feb. 21, 2014).

IV. Findings

- CDRH scientists and doctors raised concerns to Congress, the OSC, and President Obama's transition team about pressure from management to approve medical devices they believed were unsafe.

- Despite the extensive scope of the monitoring, there was insufficient written authorization, no monitoring policy in place, and there was no legal guidance given to the contractors who conducted the monitoring. The lack of any legal guidance to limit the monitoring program resulted in FDA capturing protected communications.

- Although FDA claimed to be investigating a specific leak of 510(k) information, the computer monitoring did not include a retrospective inquiry into any of the scientists' network activities. When interviewed, FDA managers and IT professionals failed to explain clearly how the rationale offered to justify the monitoring (investigating a past leak) was consistent with the method used (monitoring current activity). The goal of monitoring was allegedly to identify who leaked confidential information. Instead of looking back at previous communications using available tools in their possession, however, the FDA chose real-time monitoring of current and future communications. Because FDA managers lacked formal investigative training and did not understand the legal concerns related to employee monitoring, they believed all employee communications that occurred on government computers were "fair game."

- Because FDA managers lacked formal investigative training and legal guidance, they did not understand the legal limits of permissible employee monitoring. As a result, the scope was limited only by the FDA's technical capabilities. For example, those conducting the monitoring said they believed all employee activity having any remote nexus to government computers was "fair game"—even to the point of forensically recovering deleted files from personal storage devices when plugged into FDA computers. Moreover, the monitoring software collected all keystrokes on the computers, including the passwords for personal email accounts and online banking applications, even though *de minimis* personal use is permitted.

- The monitoring program began when a law firm representing a manufacturer alleged unlawful disclosures were made to the press regarding a device that was under FDA review. Ruth McKee first ordered monitoring on Dr. Smith's computer because Dr. Smith was believed to be the source of the leak. Later, monitoring expanded to include four additional CDRH scientists. Officials used Spector 360, a software package that recorded user activity with powerful capture and analysis functions, including real-time surveillance and keystroke logging.

- The FDA's surveillance was not lawful, to the extent that it monitored communications with Congress and the Office of Special Counsel. Federal law protects disclosures to OSC and Congress.

- HHS OIG denied FDA's repeated requests for an OIG investigation into the allegedly wrongful disclosures. OIG found no evidence of criminal conduct on the part of any employee. Still, officials continued to contact OIG to request an investigation. OIG again denied the request, and the Justice Department declined to take action.

- The monitoring program ultimately failed to identify who leaked information to the *New York Times* or the *Wall Street Journal*, despite capturing approximately 80,000 documents and inadvertently publishing those documents on the Internet.

- Despite known complaints about performance issues regarding Dr. Robert Smith, FDA management and leadership chose to address Dr. Smith's employment status through repeated requests for criminal investigation, rather than by simply taking administrative or managerial actions directly within its own control and authority.

- Over a year after receiving directives from OMB, OSC, and the FDA Commissioner, the FDA produced interim guidelines on monitoring procedures in September 2013. The FDA's interim policies require written authorization prior to initiating employee monitoring. Only the Commissioner, Deputy Commissioner, or the Chief Operating Officer can authorize surveillance of employees. The FDA has not yet implemented permanent policies to govern employee monitoring.

- The FDA's interim policies do not provide safeguards to protect whistleblowers from retaliation. Under these policies, protected communications are still subject to monitoring and may be viewed by agency officials.

V. Recommendations

Based on its investigation, the Committees identified several recommendations that, if implemented, would assist other Executive Branch departments and agencies in avoiding a repeat of the mistakes made by the FDA:

- The FDA should promptly develop permanent written procedures to govern employee monitoring and safeguard protected communications through substantive restrictions on the scope of surveillance that can be authorized on employees. Procedural safeguards merely requiring approval of surveillance by senior officials are not enough.

- The FDA should ensure that programs used to monitor employees do not collect personal information such as bank account numbers or passwords for personal e-mail accounts.

- The FDA's interim guidance does not include provisions to protect employees against retaliation if communications with Congress, the OSC, or personal attorneys are captured through monitoring. The FDA should establish procedures that ensure protected whistleblower communications cannot be used for retaliation.

- The FDA should develop clear guidance for identifying and filtering protected communications so that protected communications are not retained or shared for any reason. Any employee or contractor involved in the monitoring process, including the Review Committee established by the September 26, 2013 Staff Manual Guide, should be trained on these procedures.

- Employees should be notified that their communications with Congress and the OSC are protected by law.

- The OSC should modify its June 20, 2012 memorandum to all federal agencies regarding monitoring policies to include communications with Congress.[24]

- The GAO should conduct a study of all Executive Branch departments and agencies to determine whether the guidelines set forth for computer monitoring in the OSC's June 20, 2012 memorandum have been implemented.

[24] Memorandum from Carolyn Lerner, Special Counsel, U.S. Office of Special Counsel to Executive Branch Departments and Agencies, *Agency Monitoring Policies & Confidential Whistleblower Disclosures to the Office of Special Counsel & to Inspectors General* (June 20, 2012) [hereinafter Lerner Memo].

VI. Background

FINDING:	CDRH scientists and doctors raised concerns to Congress, the OSC, and President Obama's transition team about pressure from management to approve medical devices they believed were unsafe.

The Food and Drug Administration (FDA), a component of the U.S. Department of Health and Human Services (HHS), is responsible for promoting public health.[25] Specifically, the FDA is charged with regulating and supervising a variety of consumer health products.[26] These products include dietary supplements, prescription and over-the-counter drugs, vaccines, biopharmaceuticals, and medical devices.[27] The FDA has broad powers for determining the safety, risks, marketing, advertising, and labeling of these products.[28]

The Center for Devices and Radiological Health (CDRH) is a division within the FDA.[29] The CDRH is also tasked with protecting and promoting public health.[30] The mission of the CDRH is to ensure that patients and providers of health services have access to safe medical devices, such as hip implants, heart valves, and mammography machines.[31] The CDRH tests and examines potential medical devices, and makes recommendations to the FDA regarding the approval and widespread usage of radiation-emitting products.[32] The CDRH seeks to assure consumer confidence in devices manufactured in the United States.[33] Scientists and doctors who work for the CDRH are directly involved in product testing, making recommendations to the FDA, and assessing whether the medical devices are safe for public use.[34]

In 2007, CDRH scientists first started raising concerns about the FDA's marketing of unsafe medical devices used to detect cancers of the breast and colon.[35] These scientists also complained of a toxic work environment in which they feared retaliation by their managers for writing unsupportive reviews of medical devices they believed to be unsafe.[36] The scientists argued that the CDRH's process for approving medical devices for public use was not sufficiently rigorous and that the FDA's premature release of products without sufficient testing posed health risks to the public.[37] In an attempt to implement more stringent guidelines for this

[25] FDA, *About FDA*, http://www.fda.gov/AboutFDA/default.htm (last visited Feb. 21, 2014).
[26] FDA, *About FDA: What Does FDA Regulate?*, http://www.fda.gov/aboutfda/transparency/basics/ucm194879.htm (last visited Feb. 21, 2014).
[27] *Id.*
[28] FDA, *About FDA: What Does FDA Do?*, http://www.fda.gov/AboutFDA/Transparency/Basics/ucm194877.htm (last visited Feb. 21, 2014).
[29] FDA, *Training & Continuing Education: CDRH Learn*, http://www.fda.gov/Training/CDRHLearn/default.htm (last visited Feb. 21, 2014).
[30] *Id.*
[31] *Id.*
[32] *Id.*
[33] FDA, *About FDA: CDRH Mission, Vision & Shared Values*, http://www.fda.gov/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDRH/ucm300639.htm (last visited Feb. 21, 2014).
[34] *Id.*
[35] CDRH Letter, *supra* note 4.
[36] *Id.*
[37] *Id.*

testing process, the CDRH scientists filed complaints with the OSC,[38] the HHS OIG, Congress,[39] and even the transition team for then-President-elect Obama.[40]

On January 13, 2009, the *New York Times* published an article stating that "front-line agency scientists believed that FDA managers [had] become too lenient with the industry."[41] The article further stated that "an agency supervisor improperly forced them to alter reviews of [a] breast imaging device."[42] The article, citing internal FDA documents, referred specifically to the ongoing review of the iCAD SecondLook Digital Computer-Aided Detection System for Mammography device.[43] The article further stated:

> One extensive memorandum argued that FDA managers had encouraged agency reviewers to use the abbreviated process even to approve devices that are so complex or novel that extensive clinical trials should be required. An internal review said the risks of the iCAD device included missed cancers, "unnecessary biopsy or even surgery (by placing false positive marks) and unnecessary additional radiation."[44]

Later that day, Ken Ferry, the Chief Executive Officer of iCAD, wrote a letter to the CDRH Ombudsman, Les Weinstein, urging him to look into the breach of confidentiality concerning the pre-market approval of iCAD's breast-imaging device.[45] Ferry reminded the Ombudsman that the FDA cannot release confidential information submitted to the FDA as part of a premarket approval application, including any supplements to the application, without

---

[38] The U.S. Office of Special Counsel is the first step in the whistleblower review process. OSC is an independent federal investigative and prosecutorial agency. Its primary goal is to safeguard all protected employees from prohibited personnel practices, especially reprisal for whistleblowers. U.S. Office of Special Counsel, *Introduction to OSC*, http://www.osc.gov/Intro.htm (last visited Feb. 21, 2014); NWC Letter, *supra* note 4; CDRH Letter, *supra* note 4.

[39] Employees who provide information to Congress are protected by the Whistleblower Protection Act (WPA). *See* 5 U.S.C. § 7211. The WPA provides statutory protections for federal employees who make disclosures reporting illegal or improper activities, including employees who provide information to Congress. *See id.*; Eric A. Fischer, Cong. Research Serv., Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions, at 16 (June 20, 2013) ("A reasonable argument could be made that monitoring the content of every employee communication is excessively intrusive."). Additionally, the Fourth Amendment protects individuals from unreasonable searches and seizures. U.S. CONST. Amend. IV. states, in pertinent part: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." The Supreme Court recognizes individuals do not lose Fourth Amendment rights merely because they work for the government as opposed to a private employer. *See City of Ontario v. Quon*, 560 U.S. 746; 130 S. Ct. 2619 (2010).

[40] CDRH Letter, *supra* note 4; NWC Letter, *supra* note **Error! Bookmark not defined.**4; Telephone Call with Leslie W. Hollie, Supervisory Special Agent, Office of Investigations, Office of Inspector Gen., HHS (May 26, 2009); Letter from CDRH Scientists, CDRH, FDA, to John D. Podesta, Presidential Transition Team (Jan. 7, 2009).

[41] *Rush to Approve Devices*, *supra* note 1.

[42] *Id.*

[43] *Id.*

[44] *Id.*

[45] Letter from Ken Ferry, Pres. & Chief Exec. Officer, iCAD, to Les Weinstein, Ombudsman, CDRH, FDA (Jan. 13, 2009) [hereinafter Ferry Letter].

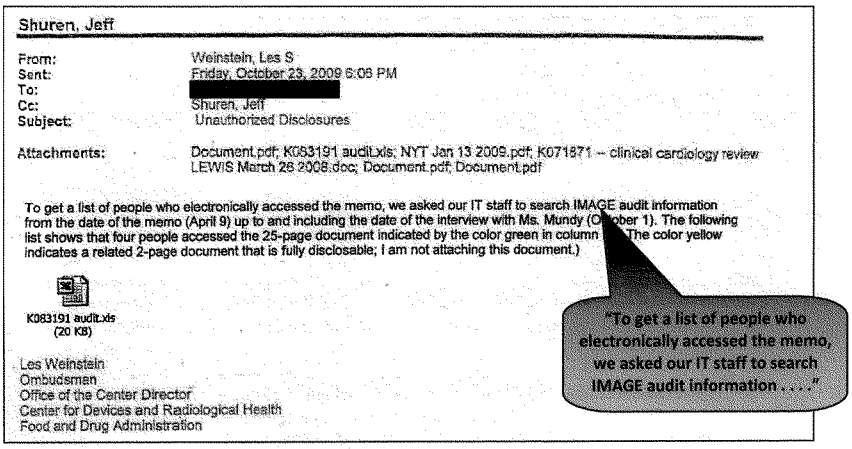
explicit permission.[46] Rather than taking any steps to deal with the issue directly, CDRH managers forwarded the complaint to the OIG.[47]

Ferry also noted that a *New York Times* reporter had called him four days before the article was published.[48] The reporter had questions concerning an internal dispute at the CDRH, which was reviewing iCAD's application.[49] According to Ferry's letter, the reporter told Ferry that the proprietary documents "were sent [to the reporter] by Scientific Officers of the FDA."[50]

On October 1, 2009, Dr. Jeffrey Shuren, Director of the CDRH, talked to a reporter about a different medical device.[51] Dr. Shuren learned that the reporter was also in possession of similar documents related to the pre-market medical device process.[52] To better understand who may have provided the information, the CDRH asked its IT Department to compile a list of those scientists that accessed a certain working memo that would either approve or reject the device under review.[53]

---

[46] *Id.*
[47] Memorandum from Les Weinstein, Ombudsman, CDRH, FDA, *Documents Related to the Radiological Devices Branch* (Mar. 23, 2009).
[48] Ferry Letter, *supra* note 45.
[49] *Id.*
[50] *Id.*
[51] Weinstein E-mail, *supra* note 16.
[52] *Id.*
[53] *Id.*



Shuren, Jeff

From: Weinstein, Les S
Sent: Friday, October 23, 2009 6:06 PM
To: [redacted]
Cc: Shuren, Jeff
Subject: Unauthorized Disclosures

Attachments: Document.pdf; K083191 audit.xls; NYT Jan 13 2009.pdf; K071871 -- clinical cardiology review LEWIS March 26 2008.doc; Document.pdf; Document.pdf

To get a list of people who electronically accessed the memo, we asked our IT staff to search IMAGE audit information from the date of the memo (April 9) up to and including the date of the interview with Ms. Mundy (October 1). The following list shows that four people accessed the 25-page document indicated by the color green in column [illegible]. The color yellow indicates a related 2-page document that is fully disclosable; I am not attaching this document.)

K083191 audit.xls (20 KB)

Les Weinstein
Ombudsman
Office of the Center Director
Center for Devices and Radiological Health
Food and Drug Administration

"To get a list of people who electronically accessed the memo, we asked our IT staff to search IMAGE audit information . . . ."

CDRH officials forwarded four names resulting from this search to the Office of Inspector General.[54] Dr. Shuren testified that he "did not recall" if the OIG was going to look into the matter.[55]

On March 28, 2010, the *New York Times* published a second article regarding the FDA's approval process for medical devices.[56] This second article, published fourteen months after the January 2009 article, cited information concerning a GE Healthcare device under FDA review:

> Scores of internal agency documents made available to The New York Times show that **agency managers sought to approve an application by General Electric to allow the use of CT scans for colon cancer screenings over the repeated objections of agency scientists**, who wanted the application rejected. It is still under review.[57]

On April 16, 2010, GE Healthcare's outside legal counsel wrote to Dr. Shuren to request an internal investigation and a meeting to discuss a possible breach of confidentiality regarding GE Healthcare's device under FDA review.[58] The letter stated:

> GE Healthcare is extremely concerned about this violation of confidentiality and respectfully requests that you conduct an internal investigation into how this information was leaked to the press.[59]

---

[54] *Id.*
[55] Shuren Tr. at 14.
[56] *F.D.A. Ignored Radiation Warnings*, *supra* note 2.
[57] *Id.* (emphasis added).
[58] Letter from Edward M. Basile, Partner, King & Spalding LLP, to Jeffrey E. Shuren, Dir., CDRH, FDA (Apr. 16, 2010) [hereinafter Basile Letter].

In light of the two *New York Times* articles describing internal turmoil at the FDA, as well as complaints filed by both iCAD and GE Healthcare, the FDA began real-time monitoring of CDRH employees' computer activity.

A. Confidential Documents are Posted Online

In May 2012, an HHS contractor, Quality Associates, Inc (QAI), posted approximately 80,000 pages of documents associated with the FDA employee monitoring on a public internet site.[60] Included in these materials were confidential and proprietary FDA documents, as well as confidential communications between FDA employees and Congress, OSC, and personal attorneys.[61] FDA had asked the HHS Program Support Center (PSC) to use a contractor to produce and print PDF-versions of the surveillance records, and PSC tasked contractor QAI with the project.[62]

After the documents left FDA, they followed a chain of custody that included several parties before they got to QAI.[63] According to HHS, QAI received the job from PSC on May 2, 2012, and completed it on May 9, 2012.[64] The files were uploaded to the site at the direction of PSC, on May 3, 2012.[65] They were removed from the site and archived six days later on May 9, 2012.[66] During this time, confidential and proprietary information was publically available and easily searchable.[67]

QAI officials claimed they were simply following their client's instructions.[68] In fact, FDA did not mark the documents as confidential, and there is no written record reflecting the sensitive nature of the documents.[69] Furthermore, the purchase order, which was submitted to the Government Printing Office (GPO) only after the work was completed, failed to mention any sensitive classification.[70] When prompted on the purchasing order form, PSC checked the "no" boxes, indicating there was 1) no personally identifiable information (PII), 2) no classified information, and 3) no sensitive but unclassified (SBU) information contained in the files.[71] HHS identified the misclassification as a "clerical error at the PSC."[72]

---

[59] *Id.*
[60] Letter from Jim R. Esquea, Assistant Sec'y for Legis., U.S. Dep't of Health & Human Servs., to Hon. Charles E. Grassley, Ranking Member, S. Comm. on Judiciary (March 13, 2013) [hereinafter Esquea Letter].
[61] NWC Letter, *supra* note 4.
[62] Esquea Letter, *supra* note 60.
[63] *Id.*
[64] *Id.*
[65] Letter from Paul Swidersky, President, CEO, Quality Associates Inc., to Hon. Charles E. Grassley, Ranking Member, S. Comm. on Judiciary (July 17, 2012).
[66] *Id.*
[67] *Id.*
[68] *Id.*
[69] *See id.*; *see also* Esquea Letter, *supra* note 60.
[70] DHHS, FDA, *GPO Simplified Purchase Agreement Work Order Form 4044* (May 23, 2012).
[71] *Id.*
[72] Esquea Letter, *supra* note 60.

FDA did not take responsibility for the mishandling of the documents.[73] Rather, FDA shifted the responsibility to HHS, which, in turn, attempted to blame QAI:

> The PSC advised QAI that the documents were sensitive and that access to them should be limited. The PSC further requested that QAI delete all files on its computers after completing the job, and shred any printed documents in its possession. Regrettably, despite these instructions, QAI's unauthorized use of an unsecure website caused QAI to lose control of the confidential material.[74]

FDA and HHS refused to take responsibility for the mishandling, even though they failed to identify the documents as sensitive or confidential in the paperwork provided to the contractor. This raises doubt about the veracity of the claim that the agencies had notified QAI of the sensitive nature of the documents. The incorrect purchase order that was submitted to GPO was dubbed by HHS as "erroneous" and was prepared after the project's completion.[75] HHS also pointed to shortcomings in the GPO form itself:

> Unfortunately, the GPO's required Work Order forms do not reflect the variety of confidential material frequently handled by Executive Branch agencies, including material as to which Congress has imposed specific statutory protections. The forms provide only three document category options[.] . . . Other options for identifying protected information, such as confidential commercial information, are not available on GPO's Work Order form.[76]

However, the documents clearly contained personally identifiable information, and yet the form incorrectly indicated that there was no such information.

VII. Authorization and Instructions for Monitoring

FINDING: Despite the extensive scope of the monitoring, there was insufficient written authorization, no monitoring policy in place, and there was no legal guidance given to the calibrators who conducted the monitoring. The lack of well-understood controls for the monitoring program caused the FDA to capture protected communications.

[73] *Id.*
[74] *Id.*
[75] *Id.*
[76] *Id.*

FINDING: Despite the fact that FDA claimed to be investigating a specific leak of 510(k) information, the computer monitoring did not include a retrospective inquiry into any of the scientists' network activities. When interviewed, FDA managers and IT professionals failed to explain clearly how the rationale offered to justify the monitoring (investigating a past leak) was consistent with the method used (monitoring current activity).

On April 16, 2010, Ruth McKee, Executive Officer for the CDRH, approached Dr. Jeffrey Shuren, Director of the CDRH, concerning the April 2010 letter and asking him what to do. Dr. Shuren testified:

> Q. And so how did you begin to look into the disclosure that appeared in the *New York Times?*
>
> A. Well, I asked Ruth McKee, who is my Executive Officer, were there ways in which we could identify the source of the leak, a little bit akin to what happened in October, **is there something you can sort of look for to then support for doing an investigation.** One of the challenges we also faced at the center is that normally in the past, the Office of Internal Affairs would take it, they would look into it over concerns, at least to my understanding, over interventions from Senator Grassley over concerns about the Office of Internal Affairs investigating whistleblowers. The Commissioner had previously instructed the Office of Internal Affairs not to conduct investigations, I think particularly if there was any possible criminal conduct as [it] relates to employees who had allegations against the agency. So—and a copy was also given of the complaint to the Office of Internal Affairs. They subsequently sent that to the OIG as well.[77]

Dr. Shuren testified that in his conversation with McKee, he learned that FDA Chief Information Officer Lori Davis had authorized the monitoring:

> A. [Ruth] wound up talking to the Chief Information Officer and then **told me afterwards that the Chief Information Officer had authorized computer monitoring**, thought it was serious and this was the step that should be taken.
>
> Q. Was computer monitoring something that you had suggested to Ruth?
>
> A. No.

[77] Shuren Tr. at 19-20 (emphasis added).

Q. You asked her to explore the options, and she came back with computer monitoring?

A. Not even from the option. **She spoke to Lori, and Lori authorized the monitoring. I will say that knowing of it, though, I didn't object to the monitoring.** I am not the expert for what are the circumstances to monitor a person's computer.[78]

Lori Davis, however, remembered the authorization of computer monitoring differently. She testified:

A. Well, we got the request from the center. I mean, asking on behalf of the center, the center asked, "Can you do that?"

Q. You mean Ruth runs the center?

A. Yes. **Ruth said, "Can you?" And we said, "Yes, we can."** So in my mind that was the authorization to proceed based [on] some conversation that obviously CDRH, whether or not that was Ruth or anybody else, I don't know, had with Joe Albaugh and either, you know, his staff at this point. I am assuming it's either Chris or Joe. Those conversations happened and they agreed on a course of action.

Q. **There was no written authorization?**

A. **Not that I'm aware of no.**[79]

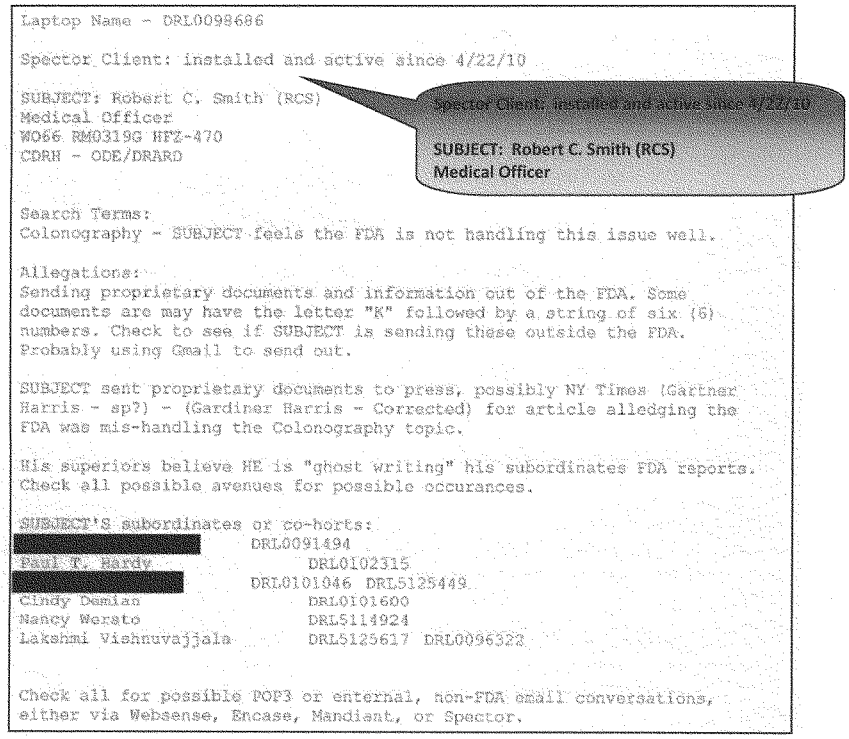
Davis further testified that she told McKee that she would forward the request for monitoring to FDA Chief Information Security Officer Joe Albaugh, who would be able to set up the monitoring.[80] For his part, Albaugh testified that he was only "a pass through between the technical team that was within [his] division and the request of the CIO and the Executive Officer."[81]

The CDRH engaged two primary investigators, Joseph Hoofnagle and Christopher Newsom, who were in place to work on the FDA's information technology security systems contract with Chickasaw Nation Industries Information Technology (CNIIT), to ultimately lead the computer monitoring effort.[82]

---

[78] *Id.* at 21 (emphasis added).
[79] H. Comm. on Oversight & Gov't Reform, Transcribed Interview of Lori Davis, at 17 (Jan. 8, 2013) (emphasis added) [hereinafter Davis Tr.].
[80] *Id.* at 9-10.
[81] H. Comm. on Oversight & Gov't Reform, Transcribed Interview of Joe Albaugh, at 9 (Mar. 7, 2013) (emphasis added) [hereinafter Albaugh Tr.].
[82] H. Comm. on Oversight & Gov't Reform, Transcribed Interview of Joseph Hoofnagle, at 6-7 (Oct. 11, 2012) [hereinafter Hoofnagle Tr.]; Newsom Tr. at 6-9.

Hoofnagle, a Contract Investigator with CNIIT who managed the Incident Response Team for the FDA's network security systems, received few instructions as to the extent of monitoring CDRH officials sought.[83] Hoofnagle's only instructions were to find documents that contained certain key words, including the letter K followed by specific numbers; such documents, which reflect the FDA's naming convention for 510(k) applications, were leaked to the press.[84] As a result, he created an initial document that would govern the investigation.[85]



Laptop Name - DRL0098686

Spector Client: installed and active since 4/22/10

SUBJECT: Robert C. Smith (RCS)
Medical Officer
WO66 RM0319G HFZ-470
CDRH - ODE/DRARD

Search Terms:
Colonography - SUBJECT feels the FDA is not handling this issue well.

Allegations:
Sending proprietary documents and information out of the FDA. Some documents are may have the letter "K" followed by a string of six (6) numbers. Check to see if SUBJECT is sending these outside the FDA. Probably using Gmail to send out.

SUBJECT sent proprietary documents to press, possibly NY Times (Gartner Harris - sp?) - (Gardiner Harris - Corrected) for article alledging the FDA was mis-handling the Colonography topic.

His superiors believe HE is "ghost writing" his subordinates FDA reports. Check all possible avenues for possible occurances.

SUBJECT'S subordinates or co-horts:
[redacted] DRL0091494
Paul T. Hardy DRL0102315
[redacted] DRL0101046 DRL5125449
Cindy Damian DRL0101600
Nancy Worsto DRL5114924
Lakshmi Vishnuvajjala DRL5125617 DRL0096322

Check all for possible POP3 or enternal, non-FDA email conversations, either via Websense, Encase, Mandiant, or Spector.

Spector Client: installed and active since 4/22/10

SUBJECT: Robert C. Smith (RCS)
Medical Officer

Hoofnagle testified that he received no legal guidance whatsoever from the FDA:

[83] Hoofnagle Tr. at 11-12.
[84] *Id.* at 12.
[85] Joseph Hoofnagle, Chickasaw Nation Industries Information Technology, *Spector Client: Installed and Active Since 4/22/10.* [hereinafter *Spector Client*].

Q. Over the course of [the monitoring], were you ever given any legal guidance about the limitations of surveillance or any legal considerations that would be relevant to using monitoring software?

A. No.

Q. At FDA, was there ever any guidance?

A. The only guidance I ever received was from law enforcement.

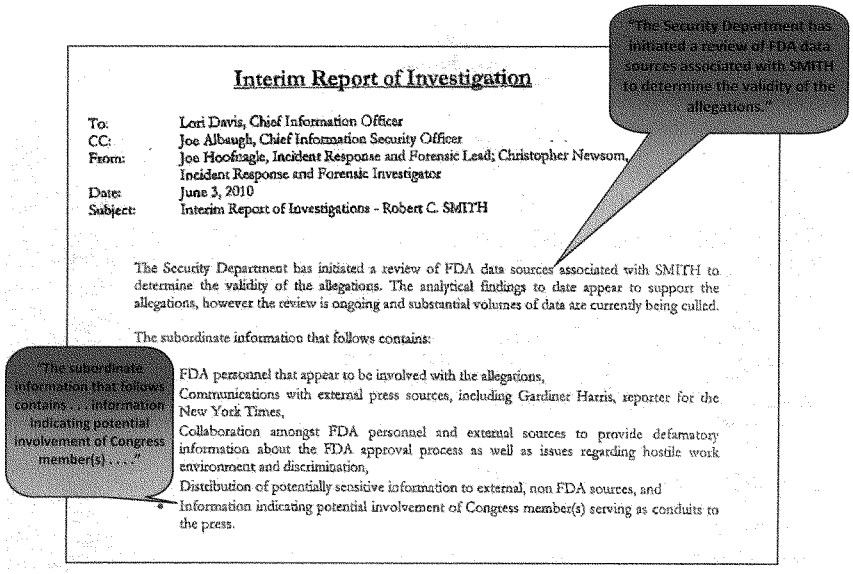
Q. Uh huh.

A. And it wasn't from a legal perspective. It was just from an authority perspective of, you know, hi, I need you to do this.[86]

In fact, CDRH leadership lacked sufficient training and background in conducting an internal investigation – particularly in monitoring computers. The contractors hired to conduct the computer monitoring received no legal guidance about the limitations of the monitoring—such as carving out communications with Congress or preserving protected attorney-client communications.[87]

After monitoring two employees' computers, contractors with CNIIT prepared an interim report to describe the status of the surveillance.[88] In the report, CNIIT contractors explained that they initiated a review of Dr. Smith's computer to determine whether he contacted external sources regarding the FDA's approval process of certain medical devices.[89]

[86] Hoofnagle Tr. at 25-26.
[87] *See, e.g.* Interim Report, *supra* note 10.
[88] *Id.*
[89] *Id.*



Interim Report of Investigation

To: Lori Davis, Chief Information Officer
CC: Joe Albaugh, Chief Information Security Officer
From: Joe Hoofnagle, Incident Response and Forensic Lead; Christopher Newsom, Incident Response and Forensic Investigator
Date: June 3, 2010
Subject: Interim Report of Investigations - Robert C. SMITH

The Security Department has initiated a review of FDA data sources associated with SMITH to determine the validity of the allegations. The analytical findings to date appear to support the allegations, however the review is ongoing and substantial volumes of data are currently being culled.

The subordinate information that follows contains:

FDA personnel that appear to be involved with the allegations,
Communications with external press sources, including Gardiner Harris, reporter for the New York Times,
Collaboration amongst FDA personnel and external sources to provide defamatory information about the FDA approval process as well as issues regarding hostile work environment and discrimination,
Distribution of potentially sensitive information to external, non FDA sources, and
Information indicating potential involvement of Congress member(s) serving as conduits to the press.

When asked about the interim report, Hoofnagle explained that the FDA officials who ordered the monitoring never voiced concerns that the information being captured was too extensive.[90] He testified:

> Q. So the very last bullet on the first page, it says, "information indicating potential involvement of Congress Member(s) serving as conduits to the press." At that point, did anybody raise a concern that information like that should not be gathered or should not be reported up to Ruth McKee?
>
> A. No.
>
> Q. Did you ever hear that concern?
>
> A. No.

[90] Hoofnagle Tr. at 36-37.

Q. Did anyone from Ruth's office ever express to you any limitations or concerns about what was being collected?

A. No.

Q. Had you ever, in your experience, you know, with monitoring initiated by the inspector general's office, heard the concern that information about communications with Congress should not be collected or should not be communicated up the chain at FDA?

A. No.

Q. How about communications with the people under surveillance and their – between them and their personal attorneys?

A. No.

Q. Between them and the Office of Special Counsel?

A. No.

Q. In any of the surveillance, were limitations or concerns expressed about the scope of monitoring?

A. No.

Q. Nobody's ever come to you and said, we should maybe limit the scope of surveillance?

A. No.[91]

Dr. Jeffrey Shuren, the highest-ranking FDA employee involved in the monitoring, was equally unaware that the monitoring had captured communications with Congress.[92] He testified:

Q. Can you explain to us why you didn't take any steps to instruct Ruth McKee to do any kind of narrowing with regard to the scope of the monitoring – once you learned that Congressional communications were being captured?

A. I mean, as I said before, it wasn't even on my radar screen. And I don't recall when I first –

Q. When it came up?

[91] *Id.*
[92] Shuren Tr. at 123.

A. I don't recall when it first came up. But, no, it just – it didn't – it just didn't dawn on me. Didn't dawn on me.[93]

The Committees found that there was no documentation or written authorization for monitoring employees' computers, and the FDA personnel interviewed were uncertain as to who authorized surveillance.

The computer monitoring also did not include a retrospective inquiry into any of the scientists' network activities to understand who may have accessed the memoranda that were leaked to the press. The FDA managers and IT professionals interviewed failed to explain clearly how the rationale offered to justify the monitoring was consistent with the method used. There appeared to be confusion about the distinction between retrospective identification of individuals who already accessed certain documentation that was featured in the *New York Times* articles and real-time monitoring going forward once the internal inquiry began. Lori Davis testified that "at that first meeting I would have said [the search for evidence of leaks on FDA computers] was historical because...in my mind it had already happened."[94]

Dr. Shuren described his concerns about both past leaks and the potential for future leaks.[95] He testified:

Q. Maybe it would be helpful for us if you clarified what exactly the purpose of the monitoring was. What was the question that you were trying to answer through the monitoring?

A. Well, again, what I...I didn't ask for monitoring. I didn't object to monitoring, but I didn't ask for monitoring. I had asked can we identify, are there ways to identify who was the source of the New York Times and the GE CT colonography device . . .

Q. So you wanted to try to figure out retrospectively who had made that leak as opposed to going forward if there were future leaks, can we kind of catch them as they occur?

A. Well, we all had concerns about future leaks. Once they were doing monitoring there was interest, are there other leaks that are occurring, but when I asked Ruth to look into what ways were available options, it was about finding the source of that.[96]

Ruth McKee, who acted as a liaison between Dr. Shuren and CNIIT, testified that "[her] understanding was there was not a technological way to do a past look" based on what she was told by the FDA Chief Information Officer, Lori Davis, and the FDA Chief Information Security

[93] *Id.*
[94] Davis Tr. at 8-11.
[95] Shuren Tr. at 32-33.
[96] *Id.*

Officer, Joe Albaugh.[97] Furthermore, McKee stated that it was her understanding that CNIIT "would be doing real time monitoring of Dr. Smith's e-mail account."[98]

Contrary to McKee's testimony, however, Christopher Newsom, CNIIT investigator, testified that although his firm had the capability to look back at e-mails that may have been sent or received in the past through FDA servers, CNIIT did not conduct such a review.[99] Newsom testified:

Q. Is there a way to look, other than looking on the hard drive, to look for e-mails. . . in the past through FDA servers?

A. Yes.

Q. Was that done with regard to Dr. Smith or Dr. Nicholas?

A. Not to my knowledge.

Q. Do you know why not?

A. I don't.[100]

Not only was there insufficient written guidance on how to monitor an employee in compliance with applicable laws, it seems there was also inadequate knowledge or guidance on how to conduct the monitoring in order to accomplish the goals of initiating the monitoring in the first place. As Dr. Shuren testified, the goal was not only to capture future leaks, but to find the past leaks linked to the *New York Times*.[101] Yet, no one conducted an inquiry into past communications.

VIII. Details of the Computer Monitoring

FINDING: The goal of monitoring was allegedly to identify who leaked confidential information. Instead of looking back at previous communications, however, the FDA chose real-time monitoring of current and future communications. Because FDA managers lacked formal investigative training and did not understand the legal concerns related to employee monitoring, they believed all employee communications that occurred on government computers were "fair game."

[97] McKee Tr. at 58-60.
[98] *Id.*.
[99] Newsom Tr. at 34-35.
[100] *Id.*
[101] Shuren Tr. at 19-20.

On April 22, 2010, the FDA began monitoring the FDA-issued computer and FDA-issued laptop of Dr. Robert Smith.[102] On May 24, 2010, the FDA began monitoring the FDA-issued computer of CDRH scientist Paul Hardy.[103] On June 30, 2010, the FDA began monitoring the FDA-issued computers of three additional CDRH scientists.[104]

To monitor these computers, the FDA used a computer monitoring software program called Spector 360, which allowed the FDA to record all computer activity in real-time. Spector 360 also has the ability to log keystrokes, capture passwords and confidential information, and record activity remotely in the event that a laptop being monitored is not directly connected to the FDA network.[105]

As part of the monitoring, the FDA took screen shots of each of the computers every five seconds and logged all keystrokes on the keyboards.[106] CDRH officials reviewed the information gathered through the monitoring using encrypted flash drives.[107] Information on the encrypted flash drives included private, non-official communications, including Gmail and Yahoo! Mail messages.[108] Transmitted information also contained communications with Congress, confidential attorney-client communications, and confidential complaints filed with the OIG and OSC.[109]

Spector 360 user activity monitoring software is readily available for both home and business use. The software "monitors, captures, and analyzes ALL user and user group activity including: e-mail sent and received, chat/IM/BBM, websites visited, applications/programs accessed, web searches, phone calls, file transfers, and data printed or saved to removal devices."[110] FDA employees received no notice that this specialized software with such extensive monitoring capability was being installed on their computers.[111] Moreover, the FDA did not routinely subject all of its employees to such intense scrutiny.[112] CNIIT investigator Joseph Hoofnagle, installed the software, and his colleague Christopher Newsom collected the data.[113] The Spector 360 software does not distinguish or filter out any information, such as protected communications with Congress, communications covered by attorney-client privilege, or communications that might otherwise be protected by law, such as confidential submissions to the Office of Special Counsel. Moreover, those collecting and forwarding the information did not have any training or instruction in minimizing the collection of privileged communications.[114]

---

[102] *Spector Client*, *supra* note 85; Ireland Letter, *supra* note 6.
[103] *See* Ireland Letter, *supra* note 6.
[104] *Id.*
[105] Newsom Tr. at 10-11.
[106] *Id.*
[107] McKee Tr. at 13.
[108] *See e.g.*, Newsom Tr. at 54-55.
[109] McKee Tr. at 76.
[110] SpectorSoft Spector 360, http://www.spector360.com (last visited Feb. 21, 2014).
[111] McKee Tr. at 73.
[112] *Id.* at 83.
[113] Newsom Tr. at 8-10.
[114] *See e.g.*, Hoofnagle Tr. at 27-28.

The CNIIT contractors collected this information and summarized it for FDA managers' later review.[115]

Ancillary Actors

10. Ned Feder – Staff Scientist / Writer – POGO (Project On Government Oversight)
1100 G Street, NW, Suite [redacted], Washington, D.C

11. [redacted] – Associate of Ned Feder
Nuclear Engineering, Texas A&M University

12. Jack Mitchell - United States Senate, Special Committee on Aging
G31 Dirksen or 628 Hart Senate Office Buildings, Washington, D.C.

13. Joan Kleinman – District Director, Congressman Chris Van Hollen (D-Md)
Office of Representative, 51 Monroe Street #507, Rockville, Md.

14. Congressman Chris Van Hollen (D-Md)
House of Representatives
1707 Longworth H.O.B., Washington, D.C.
District Office - 51 Monroe Street #507, Rockville, Md.

When asked whether they thought it was appropriate to gather attorney-client privileged communications, Hoofnagle responded:

Q. Okay. So if you got that permission and you put Spector on, and you noticed someone communicating with their personal attorney, what

A. I have not received instruction on that.

Q. Okay. You don't know what you would do.

A. You know, what I would do, I might say something. Because we're in an environment where, you know, obviously this is a problem. And I might say something. But, yeah, that process is evolving.

Q. But you don't currently have a procedure that would allow . . . you to not capture those types of communications?

[115] Chickasaw Nation Industries Info. Technologies, Actors List (May 5, 2010). [FDA 1023-1024]

A. To not capture those types of communications is correct.[116]

In order to keep the information secure, CNIIT used two encrypted flash drives to deliver information to FDA officials for review. When the CNIIT investigators found information they believed to require further review, they would flag this information when they forwarded it to FDA officials. Specifically Ruth McKee, served as the "contact point between [Office of Information Management] and the center [CDRH]."[117] McKee testified that although she had access to all the information, the information she passed on to her superiors did not contain the communications with Congress or any other protected communications.

Q. [D]id you or Mary Pastel provide summaries of the information that was being captured to either people above you in the chain of command or to the employees' supervisors?

A. Only relevant to disclosure of information, agency information.

Q. Right. To Members of Congress, to OSC?

A. No. No. Only relevant information.

Q. Why not?

A. Why not what?

Q. Well, your goal I thought was to look at disclosures to outside parties, right?

A. Right.

Q. **And nobody ever told you that it was inappropriate to look at disclosures to OSC or Members of Congress or attorneys, right?**

A. **Right.**

Q. **And you thought that was fair game because they were doing it on an FDA computer, right?**

A. **I thought monitoring was fair game.**[118]

[116] Hoofnagle Tr. at 39.
[117] McKee Tr. at 57.
[118] *Id.* at 76-77 (emphasis added).

IX. Evolution of the Monitoring Program

FINDING:	The monitoring program began when a law firm representing a manufacturer alleged unlawful disclosures were made to the press regarding a device that was under FDA review. Ruth McKee first ordered the monitoring on Dr. Smith's computer because Dr. Smith was believed to be the source of the leak. Later, monitoring expanded to include four additional CDRH scientists. Officials used Spector 360, a software package that recorded user activity with powerful capture and analysis functions, including real-time surveillance.

FINDING:	The FDA's surveillance was not lawful, to the extent that it monitored communications with Congress and the Office of Special Counsel. Federal law protects disclosures to OSC and Congress.

B. Initiation of Monitoring

FDA officials conducted surveillance of employees' computer information in response to an April 16, 2010, letter from GE Healthcare's outside counsel.[119] GE Healthcare alleged the disclosure of confidential information to the press regarding the company's premarket notification submission for a CT scanning device for colonography screening.[120] Ruth McKee, CDRH's Executive Officer, led the agency's effort to determine what it could do in response to the allegations contained in the letter, which, ultimately, was to initiate the monitoring of CDRH employees' computer activity. McKee testified:

> Q. How did it fall to you in this case to initiate the investigation?
>
> A. I think giving me credit for initiating an investigation is giving me more credit than I am due. I was the executive officer for the organization where the allegation arose. It was my job to try to figure out what options we had.[121]

The FDA's computer monitoring program appears to have been unprecedented in scope and intensity. In the past, monitoring activities were limited to activities like high-bandwidth transfers of data or viewing pornography on government computers.[122] McKee instructed Mary Pastel, Deputy Director for Radiological Health in the CDRH's Office of *In Vitro* Diagnostics and Radiological Health, to review surveillance materials collected on the encrypted flash drives. This was the first time she had received instructions to review such close surveillance of

[119] Basile Letter, *supra* note 58.
[120] *Id.* at 2.
[121] McKee Tr. at 29-30.
[122] Davis Tr. at 34.

employees' computer activity. McKee did not provide any monitoring boundaries or limitations. Pastel testified:

> Q. Okay. Had you ever been asked to do a project like that before?
>
> A. A project like what?
>
> Q. Like reviewing - from a computer that was under surveillance.
>
> A. No.
>
> Q. Did anybody give you any guidance about how to do that besides the instructions that Ruth gave you?
>
> A. No.[123]

Initially, the FDA monitored only one employee, Dr. Robert Smith. In April 2010, Lori Davis approached Joe Albaugh, who was then the FDA's Chief Information Security Officer, to set up monitoring for Dr. Smith.[124] The FDA set up monitoring of Dr. Smith on April 22, 2010, five days after FDA's receipt of the GE letter. Albaugh testified:

> Q. Can you describe for us what Lori told you?
>
> A. That . . . the executive officer had approached her and that the concern was about confidential information that had been leaked to the public.
>
> Q. And what did Lori ask you to do?
>
> A. To work with the . . . executive officer at CDRH, to set up monitoring . . . for an individual who they believed to be responsible for the leakage.
>
> Q. When you say "executive officer," can you tell us that person's name?
>
> A. That was Ruth McKee.[125]

When Davis ordered the surveillance, she offered no guidance, alternative approaches, or instructions on how to conduct the monitoring.[126] Along with the FDA officials' failure to give any instructions about appropriate protocol for the monitoring, officials also failed to offer

---

[123] H. Comm. on Oversight & Gov't Reform, Transcribed Interview of Mary Pastel, at 23 (Jan. 4, 2013) [hereinafter Pastel Tr.].
[124] Albaugh Tr. at 6-8.
[125] *Id.* at 6-7.
[126] *Id.* at 9-10.

guidance about possible legal implications of a broad-based surveillance of private information such as communications with attorneys or Congress. Pastel testified:

> Q. Did anybody talk about the legal guidelines or other things that might be worth paying attention to, such as the reason that we're kind of here today is because communications with Congress, with OSC, with some of these people's personal attorneys were captured and reviewed. And Chairman Issa and Senator Grassley were concerned about that, especially since some of Senator Grassley's staff were folks, you know, whose communications were being captured.
>
> So my question is, did anybody ever suggest to you, you know, let's exclude those communications from the scope of this review? If you see anything like that, you know, don't forward them along to whoever you were handing the material back to? Did you ever get guidance along those lines?
>
> A. **No. These were communications on government computers. And we have government computer security training every year, and in that security training it says that anything on the government computer can get monitored.**[127]

C. Type of Monitoring

Some FDA officials stated they did not fully appreciate the scope of the surveillance or the intrusiveness of the Spector 360 user activity monitoring software installed on employees' computers. While at least one FDA official was under the impression that *only* a retrospective search would be conducted to attempt to determine if an employee had leaked information to the press, another official was well aware that real-time surveillance would be the protocol used by the CNIIT investigators.

Executive Officer Ruth McKee stated:

> Q. Okay. So then what is it that you thought that IT was going to be doing in response to your request about that topic?
>
> A. I didn't know what they were going to be doing. That's why I went to talk to them.
>
> Q. Right. And after the discussion, what was your understanding of what they would be doing?

[127] Pastel Tr. at 23-24 (emphasis added).

A. That they would be doing real-time monitoring of Dr. Smith's email account.

Q. For future communications?

A. Yes.[128]

On the other hand, CIO Lori Davis maintained that she was unaware that the monitoring would include real-time surveillance. Davis stated:

Q. So, at this first meeting, did you contemplate that this would be a historical search, a search of existing e-mails in the past to determine who had been responsible for this particular leak? Or were you anticipating that there would be real-time monitoring going forward?

A. At that first meeting, I would have said it was historical . . . because in my mind, it had already happened.[129]

* * *

Q. Uh huh. So when did you understand?

A. I am going to tell you that I don't think I ever knew that they were doing real-time monitoring to the extent that it was reported on.

Q. You mean in the press?

A. In the press.

Q. So when you read the press reports about screen shots every 6 seconds

A. That's the first that I have learned the extent of what that real-time monitoring looked like.[130]

D. Development of Search Terms

Ruth McKee was responsible for determining the initial search terms for the employee computer monitoring project. The FDA's Office of Information Management (OIM) used these search terms to provide summaries and examples of the captured information to management.[131]

[128] McKee Tr. at 59.
[129] Davis Tr., at 11.
[130] *Id.* at 24.
[131] McKee Tr. at 9.

Even after the surveillance began, McKee never asked for or received any feedback from OIM about limiting or expanding the scope of the surveillance. McKee testified:

> Q. Okay. Did you ever get any feedback from Dr. Shuren or anybody else about what was being collected?
>
> A. Describe "feedback."
>
> Q. Did they give you any guidance to either limit or expand the scope of the surveillance? Did they suggest additional search terms, or did they say, keep doing what you are doing, this seems to be working?
>
> A. **No additional guidance, no. Not to expand search terms or to make changes, no.** [132]

E. Interim Report

Christopher Newsom and Joseph Hoofnagle, CNIIT investigators, drafted an interim report to summarize the status of the surveillance.[133] Prior to finalizing the interim report, CNIIT investigators met with FDA managers to review the document.[134] Little, if any, planning, however, went into the preparation of the report. Hoofnagle and Newsom did not receive any guidance on what to include. McKee testified:

> Q. In the interim report, when you met to discuss this document, did anybody have any concerns about the language that was used in here?
>
> A. No.
>
> Q. Was the language used in here – did Chris or Joe receive any guidance on how they should create this document? Were they given a framework by which to present the evidence that they uncovered?
>
> A. Not that I am aware of, no.
>
> Q. This is something they devised themselves, as far as you know?
>
> A. That is my understanding.[135]

---

[132] *Id.* at 22 (emphasis added).
[133] Hoofnagle Tr. at 34.
[134] McKee Tr. at 26-27.
[135] *Id.* at 91-92.

Newsom explained that no one at the FDA gave him any guidance on writing the report. He testified:

> Q. Did anybody give you any guidance on the language in the interim report?
>
> A. No.
>
> Q. That was all your own?
>
> A. Yes.[136]

On June 3, 2010, CNIIT sent the report to Davis and Albaugh.[137] McKee viewed the report soon after.[138] The report summarized the surveillance conducted thus far of Dr. Smith's official and personal e-mail accounts, including e-mails with journalists, congressional staff members, and the Project on Government Oversight.[139]

• Multiple Gmail contacts with Jack Mitchell (aging.senate.gov) – Emails include attachments with significant amount of documents including those self-redacted. View All instances of the above noted in order by date
• Multiple Gmail contacts with Joan Kleinman (District Director for Rep. Chris Van Hollen) – Emails include attachments with significant amount of documents including those self-redacted. View All instances of the above noted in order by date

The interim report also alleged that Dr. Smith "ghostwrote" his subordinates' reports and supplied internal documents and information to external sources.[140] The report confirmed that Dr. Smith spoke with collcagues who shared his concerns about the approval of potentially dangerous products.[141] These colleagues also worked with Dr. Smith to shed light on these alleged improprieties.[142] Prior to the issuance of the interim report, the FDA began monitoring CDRH scientist Paul Hardy's computer. Following the report, FDA officials expanded the surveillance to more CDRH employees.

---

[136] Newsom Tr. at 122.

[137] Interim Report, *supra* note 10.
[138] McKee Tr. at 26.
[139] Interim Report, *supra* note 10.
[140] *Id.*
[141] *Id.*
[142] *Id.*

F. Expansion of People Monitored

Soon after writing the interim report, monitoring was expanded to three additional CDRH employees.[143] McKee explained her role in permitting the monitoring of additional employees, acknowledging she initiated and expanded the surveillance with the approval of Dr. Shuren and others. She stated:

> Q. Okay. What was your – describe your role to me, as you understand it.
>
> A. I was essentially – I was the contact point between LIM and the center.
>
> Q. When you say you were the contact point, you initiated the scope of monitoring. Correct?
>
> A. Yes.
>
> Q. And it was your decision to expand the scope of the monitoring to the additional FDA employees, correct?
>
> A. Not only my decision, no.
>
> Q. Right. You had to seek Dr. Shuren's approval of that?
>
> A And there were discussions held, I believe, above Dr. Shuren's level.[144]

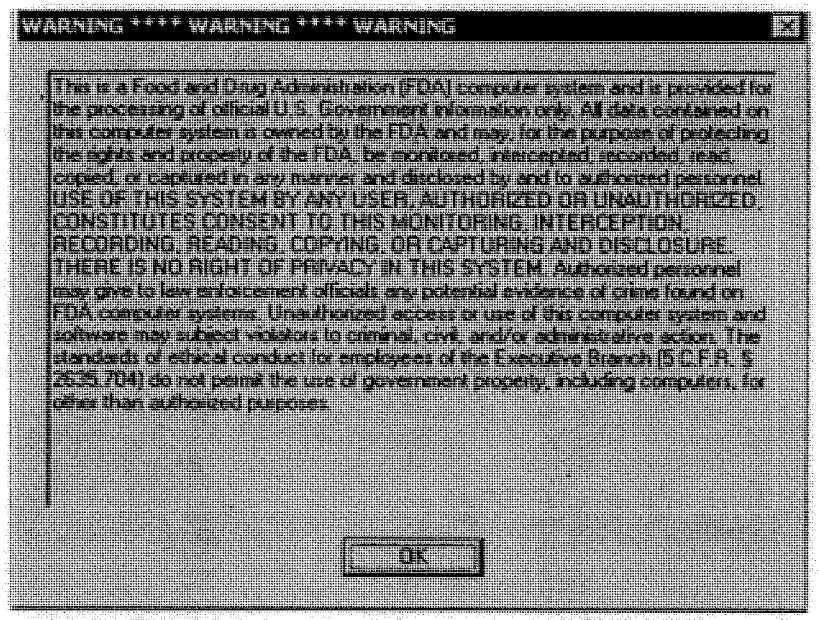
Christopher Newsom testified that fellow CNIIT investigator Joseph Hoofnagle, along with Joe Albaugh from the FDA, instructed him to expand the surveillance.[145]

G. Changes to the FDA Employee Login Disclaimer

Every employee within the FDA receives a brief login disclaimer before logging into a government computer explaining that their activities on the computer could be monitored. The FDA, however, changed the message on the disclaimer before the monitoring program began.[146] Initially, the disclaimer stated that for the purpose of protecting the FDA's property, information accessed on the computer could be "intercepted, recorded, read, copied, or captured in any manner and disclosed by and to authorized personnel."[147]

---

[143] McKee Tr. at 16.
[144] *Id.* at 57-58.
[145] Newsom Tr. at 122.
[146] Davis Tr. at 54.
[147] *Id.* at 53, Exhibit 7, FDA Employee Login Disclaimer.



In her testimony, Lori Davis, the FDA Chief Information Officer, described the purpose of the warning message.[148] She also explained that Joe Albaugh, the FDA Chief Information Security Officer, had the capacity to change the disclaimer language.[149] Davis testified:

> Q. This is the FDA warning banner. Do you recall – well, first describe to us what this is.
>
> A. This pops up when you power on your machine. It's probably one of the first things all employees see when they log onto their FDA computer.
>
> Q. And who is responsible for coming up with this text and/or making any edits or changes to the text if need be?
>
> A. Joe Albaugh worked – and I don't recall whether or not it was the Office of Inspector General that he worked with it or Office of Legal Counsel at HHS. But he worked either with OIG or Office

[148] *Id.* at 53-54.
[149] *Id.*

> of Chief Counsel – you have to ask him – on editing this language.[150]

Davis later explained that Albaugh changed the disclaimer language because he did not believe the prior language was "tight enough."[151] Although no other FDA Officials interviewed could recall when then change was made, Davis stated that Albaugh decided, to edit the message before monitoring began on CDRH scientists and doctors.[152] Davis stated:

> Q. So you recall a change in this language –
>
> A. Correct.
>
> Q. -- at some point while you were there?
>
> A. Correct.
>
> Q. Okay. Can you tell me what precipitated the change and why?
>
> A. You'll have to ask – **in Joe's mind, he felt that the language was not tight enough.**
>
> Q. When did he – he expressed that concern to you at some point?
>
> A. Yes.
>
> * * *
>
> Q. Do you recall whether it was after the monitoring in this case had already begun?
>
> A. No, it was before.[153]

Mr. Albaugh, however, could not recall any specific changes made or when they occurred, only that he was sure changes were made.[154]

According to documents obtained by the Committee, the disclaimer message was edited to explain to users that they have no reasonable expectation of privacy when using the FDA security system.[155] The prior disclaimer was significantly expanded to list specific devices which encompassed the U.S. Government information system, and outlined additional details about what information the FDA could monitor on the computer.[156] These personal storage

---

[150] *Id.*
[151] Davis Tr. at 54.
[152] *Id.*
[153] *Id.* (emphasis added).
[154] Albaugh Tr. at 34.
[155] *See* Ireland Letter, *supra* note 6.
[156] *Id.*

devices were ultimately monitored and searched in the FDA monitoring investigation. The revised disclaimer stated:

> You are accessing a U.S. Government information system, which includes (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network.
>
> This information system is provided for U.S. Government-authorized use only. Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties.
>
> By using this information, you understand and consent to the following:
>
> - You have no reasonable expectation of privacy regarding any communications or data transiting or stored on this information system. At any time, and for any lawful government purpose, the government may monitor, intercept, and search and seize any communication or data transiting or stored on this information system.
>
> - Any communications or data transiting or stored on this information system may be disclosed or used for any lawful government purpose.[157]

Regardless of when the banner was changed to address, among other things, personal storage devices that were attached to agency computers, it did not discuss the intrusive search procedures to which those personal storage devices attached to the FDA network would be subject.

In the course of the FDA monitoring investigation, CNIIT investigator Chris Newsom used Encase, a forensic imaging tool used to recover specific documents, including deleted files, artifacts, and information from unallocated space, to retrieve data from the personal storage device of one of the five employees being monitored.[158] Therefore, the employees being monitored were not only subject to real-time monitoring of activity on FDA computers, but also to an additional layer of intrusion involving personal storage devices. Encase was used to reconstruct and copy personal files that FDA employees had deleted from their personal storage device before plugging that device into an FDA computer. That level of surveillance is not reasonably contemplated by the phrase in the FDA's disclaimer, which merely asserts that a "government information system" includes "all devices and storage media attached to this network."

[157] *Id.*
[158] Newsom Tr. at 27, 63.

X. The Office of Inspector General Declines to Investigate

FINDING:	HHS OIG denied FDA's repeated requests for an OIG investigation into the allegedly wrongful disclosures. OIG found no evidence of criminal conduct on the part of any employee. Still, officials continued to contact OIG to request an investigation. OIG again denied the request, and the Justice Department declined to take action.

When Dr. Shuren learned about the extent of the confidential disclosures of Dr. Smith and other employees, he wrote to the FDA Office of Internal Affairs (IA), which in turn referred the matter to the Office of Inspector General.[159] Les Weinstein, the Ombudsman for the CDRH, contacted the OIG to request an investigation into Dr. Smith's disclosure of confidential information to the press.[160] Dr. Shuren was copied on the e-mail request to the OIG.[161] On May 14, 2010, IA wrote to the OIG in response to the allegations contained in GE Healthcare's April 16, 2010, letter.[162] In its response, IA asked the OIG to investigate any disclosure of confidential information by CDRH employees.[163]

In response, the OIG wrote to IA on May 18, 2010, stating the wrongful disclosure allegations "lack any evidence of criminal conduct on the part of any HHS employee."[164] The OIG added that federal law permits disclosures to the media and Congress when related to matters of public safety, so long as the information is not protected by national security interests or any other specific prohibitions.[165] Later, the OIG clarified the statement to mean that the OIG did not have the authority to determine the legality of such disclosures.[166] Instead, the OIG could refer matters to the Department of Justice if there were "reasonable grounds to believe" there was a criminal law violation.[167] The OIG clarified that the final determination on whether there is potential criminality was the Justice Department's responsibility.[168]

On June 28, 2010, Dr. Shuren again wrote to the OIG with a new request for an investigation.[169] He explained that the FDA had acquired new information regarding the disclosures based on an internal investigation.[170] He reiterated that the disclosures, which were prohibited by law, had continued for quite some time.[171] His letter explained that FDA officials

[159] Shuren Tr. at 14.
[160] Weinstein E-mail, *supra* note 16.
[161] *Id.*
[162] Letter from Mark S. McCormack, Special Agent in Charge, Office of Internal Affairs, FDA, to Scott A Vantrease, Office of Inspector Gen., HHS (May 14, 2010).
[163] *Id.*
[164] Vantrease Letter, *supra* note 17.
[165] *Id.*
[166] Letter from Elton Malone, Office of the Inspector Gen., HHS, to Mark McCormack, Office of Internal Affairs, FDA (Jul. 26, 2012).
[167] *Id.*
[168] *Id.*
[169] Shuren Letter, June 28, 2010, *supra* note 19.
[170] *Id.*
[171] *Id.*

conducted their own investigation because they believed an employee had leaked confidential proprietary information.[172] Dr. Shuren noted that IA authorized OIM to conduct real-time monitoring of Dr. Smith's computer.[173] He enclosed excerpts of the investigative findings and asked the OIG to review the communications to determine whether employees engaged in unlawful conduct.[174]

On November 3, 2010, the Justice Department wrote to the HHS OIG.[175] The Justice Department explained that the Criminal Division would decline prosecution.[176] The OIG concurred with the Justice Department's decision not to prosecute because "the referral lack[ed] any evidence of criminal conduct on the part of any HHS employee."[177]

On February 23, 2011, Dr. Shuren wrote for the third time to the OIG to request an investigation into two FDA employees' nonconsensual recording of phone calls and meetings regarding FDA business.[178] He added that the nonconsensual recordings were potential violations of state and/or federal wiretapping laws, which, in some instances, require consent of the parties to the communication.[179] Dr. Shuren noted that violations of wiretapping laws are felonies, which may subject the person in question to fines and imprisonment.[180] He further explained that there was no FDA policy that permitted the unauthorized recording of phone calls and employee meetings, or the use of FDA equipment for surveillance.[181] Additionally, he expressed concerns over the storage of the recordings, noting the agency's requirements for secured storage and destruction of sensitive information.[182]

In March 2011, Ruth McKee also wrote to the OIG in reference to the alleged recordings. The OIG responded to Ruth McKee on June 10, 2011, and declined to investigate the matter.[183] Rather, the OIG deferred to the FDA for any necessary administrative action.[184] Still, the monitoring continued according to Dr. Shuren:[185]

> Q. I'm trying to understand the distinction between continuing to pursue the investigative track, by which I mean monitoring, and then the administrative track, which sounds like it started shortly after you got that letter. But simultaneously the surveillance continued. Is that correct?

---

[172] *Id.*
[173] *Id.*
[174] *Id.*
[175] DOJ Letter, *supra* note 21.
[176] *Id.*
[177] Vantrease Letter, *supra* note 17; E-mail from Kenneth Marty, Special Investigations Branch, Office of Inspector Gen., Dep't of Health & Human Servs.. to Ruth McKee, Exec. Officer, Ctr. for Devices & Radiological Health, FDA (June 10, 2011, 1:37 p.m.) [hereinafter Inspector Gen. E-Mail].
[178] Shuren Letter, Feb. 23, 2011, *supra* note 16.
[179] *Id.* at 2.
[180] *Id.*
[181] *Id.*
[182] *Id.* at 1-2.
[183] Inspector Gen. E-mail, *supra* note 177.
[184] *Id.*
[185] Shuren Tr. at 41.

A. Yes.[186]

When asked about the multiple requests for an OIG investigation into the disclosures, McKee expressed disappointment at the OIG's decision not to investigate. She stated:

Q. Okay. At a number of points along the way facts, evidence was referred to the Inspector General's Office. There were a series of letters asking the IG to take up this matter. Were you surprised or disappointed or did you have any reaction when the Inspector General's Office declined?

A. Yes.

Q. Can you describe for us what that reaction was?

A. Surprised and disappointed.

* * *

Q. Why then were a series of additional efforts made to refer this to the IG after it had been declined more than once?

A. The additional referrals were for different topics.

Q. Okay. So there was a hope that while the IG had set aside the communicating proprietary information outside the agency piece of the puzzle, that maybe they would take up the patent issue or the one party recording issues?

A. Yes.

Q. And they declined at each step of the way?

A. Yes, they did.[187]

XI. Monitoring Was Not the Solution

FINDING: The monitoring program failed to identify who leaked information to the New York Times or the Wall Street Journal, despite capturing approximately 80,000 documents.

[186] *Id.*
[187] McKee Tr. at 90-91 (emphasis added).

The whole point of initiating the monitoring of the five FDA employees was to confirm the suspicions of FDA management that these employees were, in fact, leaking information to the press. At the direction of FDA officials, the monitoring program collected approximately 80,000 documents.[188] Interviews with key FDA officials made it clear that the program did not accomplish what it was set up to achieve. For example, Dr. Shuren stated:

> Q. Okay. So you never actually found proof that Robert Smith was disclosing [information] it to the press?
>
> A. Confidential information?
>
> Q. Yes.
>
> A. Not to my recollection.[189]

In fact, in an effort to be thorough, FDA officials even reviewed Dr. Robert Smith's FDA-issued computer once he left the agency following the expiration of his contract but found no evidence of disclosures of confidential information to the media.[190]

FDA management went to unprecedented lengths in order to determine who was leaking confidential information to the press. Yet, they failed to find proof of leaks to the press. In fact, the only information FDA officials uncovered on one of the five FDA scientists monitored, Paul Hardy, was information disclosed to Congress – a protected form of communication.[191]

XII. Managing By Investigation

FINDING: Despite known complaints about performance issues regarding Dr. Robert Smith, FDA management and leadership chose to address Dr. Smith's employment status through an investigation rather than by simply taking an administrative action.

Over the course of the investigation, it became evident that FDA officials chose not to address Dr. Robert Smith's job performance through administrative procedures available to them. Instead, FDA officials used the HHS OIG and computer monitoring tactics to investigate him. Dr. Robert Smith, the first scientist FDA officials monitored, was a thorn in the agency's side. According to Dr. Shuren, Dr. Smith created a "toxic" environment. Dr. Shuren stated:

> The work environment was toxic and had bled over to other parts of the center as well. And that was a – radiological devices was a hornet's nest.

[188] Newsom Tr. at 132.
[189] Shuren Tr. at 93.
[190] Newsom Tr. at 32.
[191] McKee Tr. at 17-18.

> It was essentially two camps. It was the people who were – Robert and his supporters, and there [were] other people or people who just wanted to stay out of the way.
>
> People felt intimidated to speak up. There were people who I spoke to regarding what was going on in the office and some of them, I asked if they would speak to other investigators and OIG and others. And they declined to do so. They didn't even want to talk about it.
>
> We had reviews being held up. They were just not going anywhere. And there wasn't an issue about science. Some of these were tactics of a meeting was being scheduled, and they'd say, we're not meeting – an internal meeting – until you give us an agenda. Then we want to see all e-mails between managers and the company before we actually agree to come in for an internal meeting. I mean, there was one thing – there was one thing after the other.
>
> Early on, one of the things Robert I think even put this in writing, his position was if a manager didn't have adequate experience or expertise, his perspective, and they disagreed with another scientist, that is retaliation. By its nature. I mean, those were the kind of things we were dealing with.
>
> And it was – it was constant. It was one thing after another.[192]

When asked whether FDA officials attempted to resolve this "toxic" environment through administrative measures rather than investigative channels, Dr. Shuren responded that senior management had rejected earlier attempts to discontinue Dr. Smith's contract. He stated:

> A. I mean, he had managers in different offices at different times talk to him about his bad conduct. He received a number of cautions as well.
>
> Q. These are the specific questions I want to ask about.
>
> A. . . . But we also had the management team, you have to remember. So for these managers who also want to do something, they had the Assistant Commissioner for management, they had the lawyers, the HHS lawyers from General Law Division, these are the employment lawyers, and you have labor and employee relations, and that is what that mechanism was, the managers actually were going to them about what do we do in the circumstances, and they were hearing back from those people, this is what you should be doing. It wasn't about ignoring Robert Smith at all, but they were

[192] Shuren Tr. at 43.

getting their advice on what to do, they were talking with Robert, there was memo of cautions.

* * *

Q. **So my understanding is a letter of caution is not an adverse personnel action as a technical matter.**

A. **Right.**

* * *

Q. So this group, this management group that you described, you participated in the discussions with them and with Robert Smith's managers about various steps to take?

A. No, I for the most part was not part of the managers team. I got pulled into some things a little bit more than I normally would simply because of the circumstances. **So even on the managers for Robert not wanting to renew his contract, they came to me because they were concerned about would the Office of Commissioner not let them, if you will, not renew his contract, essentially saying you have to renew it.** Two years before the managers did not want to renew Robert's contract, and the Office of Commissioner stepped in and told them you will have to renew it, **and they were worried, even though it is different people, they were worried about the same thing. So I told them, I will support you, and I went to the Commissioner's office about will they support not renewing the contract, and even that decision on not renewing the contract and the memo regarding it went all the way up to the Acting General Counsel at HHS for review.**[193]

So, according to Dr. Shuren, managers initially renewed Dr. Smith's contract even though there were significant concerns about his performance. Then, despite continued problems and a letter from the OIG deferring to the FDA to take administrative action, senior FDA officials chose to address Dr. Robert Smith's alleged shortcomings through repeated referrals to the OIG for criminal investigation, rather than through direct management action.

[193] *Id.* at 82 (emphasis added).

XIII. Post-Monitoring Changes

FINDING:	Over a year after receiving directives from OMB, OSC, and the FDA Commissioner, the FDA produced interim guidelines on monitoring procedures in September 2013. The FDA's interim policies require written authorization prior to initiating employee monitoring. Only the Commissioner, Deputy Commissioner, or the Chief Operating Officer can authorize surveillance of employees. The FDA has not yet implemented permanent policies to govern employee monitoring.

FINDING:	The FDA's interim policies do not provide safeguards to protect whistleblowers from retaliation. Under these policies, protected communications are still subject to monitoring and may be viewed by agency officials.

In response to the intrusive nature of FDA's computer monitoring, the federal government took the unprecedented step of acknowledging that excessive monitoring could violate the law. On June 20, 2012, the Office of Management and Budget (OMB) sent a memorandum urging all Executive Branch departments and agencies to review their employee monitoring policies. [194] The memorandum is the first acknowledgment by the federal government that there are limitations on surveillance of government employees' computers.

In particular, the memorandum recognizes that the government may not conduct unlimited computer surveillance, even when an employee is on duty and operating a government-owned computer.[195] Further, the memorandum also purports to safeguard protected communications made using private e-mail accounts.[196] Specifically, OMB instructed agencies to "take appropriate steps to ensure that those policies and practices do not interfere with or chill employees' use of appropriate channels to disclose wrongdoing."[197] OMB enclosed a memorandum from OSC highlighting that federal law protects whistleblowers' rights.[198]

According to OSC, while lawful agency monitoring of employee electronic communications may serve a legitimate purpose, agencies should ensure these policies and practices do not interfere with or deter employees from using appropriate channels to disclose wrongdoing.[199]

[194] Memorandum from Steven VanRoekel, OMB Fed. Chief Information Officer, & Boris Bershteyn, OMB General Counsel, *Office of Special Counsel Memorandum on Agency Monitoring Policies and Confidential Whistleblower Disclosures* (June 20, 2012).
[195] *See id.*
[196] *See id.*
[197] *Id.*
[198] *See id.*
[199] Lerner Memo, *supra* note 24.

OSC addressed the issue of electronic monitoring and protected communications with OSC and OIGs.[200] The memorandum failed, however, to acknowledge whistleblowers' rights to communicate with Congress.[201] OSC issued a press release on February 15, 2012, acknowledging that monitoring employee e-mails should not dissuade employees from making disclosures to Congress.[202] Unlike the OSC memorandum, however, the press release was not circulated government-wide and did not receive as much attention. As a result, agencies have not received official notice from OMB or OSC that computer monitoring guidelines should ensure that protected communications include communications with Congress. If the Executive Branch has a legitimate reason for excluding communications with Congress from those that should be protected, it has not explained what that reason might be.

On September 24, 2012—shortly after OSC released its memorandum—FDA Commissioner Margaret Hamburg directed Elizabeth Dickinson, the FDA Chief Counsel, to alert the agency that future installation of Spector 360 software would require "written approval by the FDA Chief Counsel or her delegee."[203] Commissioner Hamburg also directed the CIO and Chief Counsel to "promptly" develop written standards and procedures for monitoring employee personal work computers.[204]

Despite the urgency expressed by the Commissioner, FDA did not release any additional guidelines until over a year later. On September 26, 2013, Chief Operating Officer (COO) and Acting Chief Information Officer (CIO) Walter Harris released interim guidelines outlining new procedures for employee monitoring.[205] The interim guidelines have not yet been fully implemented, and are subject to change as the FDA continues to develop policies that are consistent with HHS monitoring policies. The FDA Commissioner's September 2012 memorandum, therefore, still acts as the guiding document. The interim guidelines included the following:

- Basis for computer monitoring
- Express written authorization
- Establishment of a review committee
- Limitations on time, scope, and invasiveness
- Periodic review by the COO
- Legal review of monitoring requests by FDA Office of the Chief Counsel[206]

---

[200] *Id.*
[201] *Id.*
[202] U.S. Office of Special Counsel, Press Release, *Office of Special Counsel Opens Investigation into FDA's Surveillance of Employees' E-mail* (Feb. 15, 2012).
[203] Memorandum from Elizabeth Dickinson, FDA Chief Counsel, *Requirements for Deploying Spector Software* (Aug. 1, 2012).
[204] Memorandum from Margaret A. Hamburg, FDA Commissioner to Walter A. Harris, FDA Chief Operating Officer, Eric Perakslis, Chief Information Officer, & Elizabeth H. Dickinson, FDA Chief Counsel, *Monitoring of FDA Personnel Work Computers* (Sept. 24, 2012).
[205] FDA Information Resources Management – Information Technology Security, *Monitoring of Use of HHS/FDA IT Resources* (Sept. 26, 2013).
[206] *Id.*

Although FDA's interim policies propose to establish procedures for regulating employee monitoring, the policies do not provide protections against whistleblower retaliation. Even with national media attention, recommendations from outside agencies, and internal agency directives, FDA has yet to implement permanent policies and procedures. Additionally, as of the date of this report, multiple inquiries are still pending, including two OIG reviews requested by the Secretary of HHS.

XIV. Conclusion

The FDA's secret monitoring of CDRH employees is a prime example of a flawed oversight process for employee computer surveillance. A federal agency may monitor employees' computers for a lawful purpose. Retaliatory motives and excessively intrusive monitoring schemes that capture legally protected communications, however, are inappropriate.

The lack of appropriate limitations and safeguards in conducting employee surveillance has long been a concern of the Committee on Oversight and Government Reform. In 2012, the Committee learned of a similarly flawed employee surveillance program at the Federal Maritime Commission (FMC). Like the FDA, the FMC used Spector 360 to conduct covert surveillance of a select group of employees. The FMC allegedly targeted for surveillance employees who expressed opinions which contradicted the Chairman's views. Furthermore, the FMC OIG requested that agency management stop using the monitoring software, citing concerns it violated federal privacy regulations. Despite this admonition, agency management continued using Spector 360 against the advice of the Inspector General. The Committee found that these tactics, along with adverse personnel decisions, contributed to a climate of fear and intimidation among agency managers and staff.[207]

The Committees' investigation of the FDA's surveillance of whistleblowers raises broader questions about the policies and practices for electronic surveillance at other Executive Branch departments and agencies. In this instance, scientists and doctors raised concerns about the effectiveness of the FDA's process for approving medical devices. Once they learned that scientists and doctors had communicated with Congressional offices and the Office of the Special Counsel, FDA officials did not have a legitimate purpose to institute an intrusive monitoring scheme that would capture those communications, among others. The FDA officials who conducted employee monitoring appeared to be engaged in a form of retaliation, as well as an attempt to interfere with protected whistleblower communications. These actions may have serious ramifications, as they threaten to chill legally protected disclosures to Congress and the Office of Special Counsel. While the FDA has adopted interim policies to regulate surveillance of employees' computers, there are still no permanent guidelines in place. Additionally, the temporary regulations do not provide safeguards to protect whistleblowers from retaliation.

[207] Letter from Hon. Darrell E. Issa, Chairman, H. Comm. on Oversight & Gov't Reform, to Richard A. Lidinsky, Jr., Chairman, Fed. Maritime Comm'n (May 9, 2012).

From the start, when the FDA learned of the potential disclosures to entities outside of the FDA, officials who ordered the monitoring demonstrated an egregious lack of oversight and judgment. There were no guidelines in place, and no one considered the consequences of an invasive monitoring scheme. An agency may not monitor whistleblowers to retaliate against those whose actions were lawful. Here, the scientists and doctors who raised concerns about the FDA's approval process in good faith were within their lawful right to do so.

Testimony from numerous FDA officials established that when officials ordered the surveillance, they failed to consider the legality and propriety of the monitoring. Instead, officials not only approved the monitoring, but also expanded both the number of CDRH employees monitored and the scope of the monitoring. Witnesses also testified that the officials who ordered the monitoring were not adequately aware of the intrusiveness of the computer monitoring software. When FDA officials later contacted OIG to request an investigation into the whistleblowers' release of unauthorized information, OIG declined to investigate because the allegations were unsubstantiated. Despite OIG's response, monitoring of employees continued.

The Committee on Oversight and Government Reform of the U.S. House of Representatives has jurisdiction over the federal civil service, government management, and the management of government operations and activities, as set forth in House Rule X. In addition to its role in conducting oversight and consideration of nominations, the Senate Judiciary Committee also considers other matters, including government information, as set forth in the Standing Rules of the Senate. The Oversight and Government Reform Committee and the Senate Judiciary Committee have a responsibility to ensure federal agencies are using taxpayer dollars appropriately and upholding whistleblower protection laws.

Executive Branch departments and agencies must take a cautious approach to employee monitoring. An intrusive monitoring scheme may run afoul of federal law. In addition, such a scheme could have a chilling effect, making employees reluctant to report waste, fraud, abuse, and mismanagement for fear of retaliation. The Committees will continue to assess whether the FDA is taking adequate steps to prevent such practices from recurring, and will endeavor to determine whether other Executive Branch departments and agencies are taking appropriate steps to engage only in limited employee monitoring when absolutely necessary, subject to thorough vetting and approval.