Ballard Spahr
LLP

Report of Independent Investigation

Regarding Remote Monitoring of Student Laptop Computers by the Lower Merion School District

May 3, 2010

TABLE OF CONTENTS

I. INTRODUCTION AND SUMMARY OF FINDINGS

On February 19, 2010, the Board of School Directors ("Board") of the Lower Merion School District ("LMSD" or the "District") retained Ballard Spahr LLP to conduct an independent investigation into the District's remote monitoring of laptop computers that the District issued to its high school students, and to report the results of its investigation to the Board and make appropriate recommendations. We hereby submit this Report of the results of our investigation to the Board.

Following a comprehensive, 10-week investigation that included the review of approximately 500,000 pages of documents; 42 interviews of LMSD directors, administrators, and employees; interviews of other witnesses with potentially pertinent knowledge; and the receipt of a report from L-3 Services, Inc. ("L-3" and the "L-3 Report"), an independent computer forensic consulting firm, we find:

- In the Fall of 2007, the District purchased LANrev, a comprehensive computer systems management software application that allowed the District's Information Services ("IS") Department personnel to install software, disseminate software updates and patches, and otherwise maintain thousands of District computers remotely from a central server, eliminating the need to service each computer individually. LANrev included a feature called "TheftTrack," which, when activated for a particular computer, was capable of recording at a set interval: (i) the Internet Protocol ("IP") address at which the computer was connected to the Internet; (ii) a photograph taken by the computer's Web camera ("webcam") of whatever was in front of the webcam; and (iii) an image reflecting whatever was on the computer's screen (a "screenshot"). The feature was not capable of recording audio or video. Nor did it allow a user to take a remote webcam photograph or screenshot on command at a given moment; once activated, the collection of images was automated. TheftTrack was one of several features that IS Department personnel considered in choosing LANrev over other available computer systems management applications; it was not the primary reason they chose LANrev.

- The District launched its One-to-One laptop program at the beginning of the 2008-2009 school year at Harriton High School ("HHS") and at the beginning of the 2009-2010 school year at Lower Merion High School ("LMHS"). Pursuant to the program, the District issues to each of its approximately 2,300 high school students an Apple MacBook laptop for use during the school year. The laptops have integrated webcams in the bezels of their screens. Like other computers used throughout the District by administrators, teachers, and students, the One-to-One program laptops ran the LANrev client software that enabled them to communicate with the LANrev server when connected to the Internet.

- Students and their parents or guardians were required to sign the District's guidelines concerning the acceptable use of LMSD's local network. Those guidelines – which were prepared several years before the District launched the One-to-One initiative – do not address the issues specifically raised by the issuance of laptops to students, including the existence or capabilities of the LANrev TheftTrack feature. Families able to pay also were required to pay annual insurance fees and insurance deductible payments in the event of laptop theft or damage. The District's communications about the insurance requirements also did not disclose the existence or capabilities of TheftTrack.

- The District likewise did not adopt official policies or procedures governing use of the TheftTrack feature by IS personnel. Instead, the IS Department developed its own procedures that varied over time and were not followed consistently. Recordkeeping also was informal and inconsistent.

- Two members of the IS Department had LANrev administrator permissions that allowed them to activate TheftTrack. As a general matter, they activated tracking for a particular laptop only if they received an instruction to do so from a school administrator or IS staff member who received a report from the student that his or her laptop was missing or lost. In at least one instance, however, tracking by webcam photograph and screenshots was activated for a laptop for which the student's family had outstanding insurance bills. And in a number of instances, tracking was allowed to remain activated – sometimes for extended periods – even after the laptop was found or recovered.

- Analysis of all of the available forensic data and other evidence collected during the investigation reveals that: (i) TheftTrack was activated 177 times on One-to-One program laptops during the 2008-2009 and 2009-2010 school years; (ii) 101 (57%) of those activations involved use only of the IP address-tracking feature, meaning that such activations did not result in the collection of any images (*i.e.*, webcam photographs or screenshots); (iii) as a result of the activations that could have resulted in the collection of images from One-to-One program laptops, electronic copies of 30,564 webcam photographs and 27,428 screenshots existed in IS Department systems as of February 23, 2010 (the date on which the LANrev server was shut down at the outset of our investigation); and (iv) the vast majority (87%) of the images recovered resulted from the failure to deactivate TheftTrack on 12 laptops after they had been found or recovered.

- Notwithstanding the large quantity of images collected by LANrev TheftTrack, we found no evidence that the feature was used to "spy" on students. Although there is no forensic method to determine with certainty how often images stored on the LANrev server were viewed, we found no evidence that any District personnel surreptitiously downloaded images from the LANrev server. Rather, the collection of images from laptops while they were in the possession of students resulted from the District's failure to implement policies, procedures, and recordkeeping requirements and the overzealous and questionable use of technology by IS personnel without any apparent regard for privacy considerations or sufficient consultation with administrators.

- There is no evidence that the members of LMSD's Board or top-level District administrators (including the Superintendent, Assistant Superintendent, and the principals and assistant principals of HHS and LMHS) knew how TheftTrack worked or understood that it could collect large quantities of webcam photographs or screenshots from unsuspecting students and their laptops. To the limited extent that certain of them received indications of the IS Department's ability to "track" student laptops, those individuals did not appreciate the potential of that ability to raise serious privacy concerns, and they should have sought more information about TheftTrack from IS personnel and/or advice from the District solicitor. And, IS personnel should have shared the full range of TheftTrack's capabilities with administrators and/or the Board: (i) before a decision was made to implement the feature; and (ii) to obtain guidance concerning the procedures that should have been followed to protect the privacy of students and their families.

Based upon these findings, we recommend that the District take a number of steps to: (i) remedy the deficiencies and mistakes that compromised the privacy of students and their families; and (ii) heighten the protection of the privacy of students and their families with respect to the District's use of computer technology. Our findings and recommendations are set forth in detail below.

II. BACKGROUND

A. <u>The Events Giving Rise to the Investigation</u>

1. Civil Litigation

On February 16, 2010, Blake J. Robbins, a student at Harriton High School ("HHS"), by his parents, Michael E. and Holly S. Robbins, filed a complaint in the United States District Court for the Eastern District of Pennsylvania against LMSD, LMSD's Board, and

Christopher W. McGinley, LMSD's Superintendent (the "Robbins Complaint").[1] The District learned about the lawsuit on February 18, 2010.[2]

The Robbins Complaint alleges – on behalf of the Robbinses and a putative class "consisting of Plaintiffs and all other students, together with their parents and families . . . who have been issued a personal laptop computer equipped with a web camera . . . by [LMSD]" – that "[u]nbeknownst to Plaintiffs and the members of the Class, and without their authorization, Defendants have been spying on the activities of Plaintiffs and Class members by Defendants' indiscriminant [*sic*] use of and ability to remotely activate the webcams incorporated into each laptop issued to students by the School District."[3] Specifically with respect to Blake J. Robbins,

[1] The Robbins Complaint is reproduced in the Appendix to this Report at Tab 203. Documents reproduced in the Appendix are otherwise referred to herein with the abbreviation "App. Tab [#]." With the exception of the discussion in Section IV(G)(5), below, about our findings with respect to specific allegations made concerning Blake J. Robbins, we have not included in this Report and redacted from the documents in the Appendix information that could be used to identify individual students.

[2] In a newspaper article published after the lawsuit was filed, Ms. Robbins was quoted as saying:

> I tried to communicate with the school prior to filing the lawsuit.
>
> I didn't want to file the lawsuit; I didn't want to go through that.
>
> Nobody called me back.
>
> Nobody responded to me.

William Bender, Spycam Case More Than Meets The Eye, Philadelphia Daily News, April 28, 2010, App. Tab 199.

In our review of documents and interviews of District personnel, we found no evidence that Ms. Robbins left messages with District personnel to that effect.

[3] Robbins Compl. ¶¶ 1, 2, App. Tab 203.

the complaint alleges that on November 11, 2009, Lindy Matsko, an HHS assistant principal, "informed [Blake J. Robbins] that the School District was of the belief that [he] was engaged in improper behavior in his home, and cited as evidence a photograph from the webcam embedded in [his] personal laptop issued by the School District."[4]

The Robbins litigation is ongoing and in its early stages; the defendants have not yet formally responded to the Robbins Complaint but some discovery has been conducted.

On March 18, 2010, a group of six parents of LMSD high school students filed a motion to intervene in the Robbins case to pursue claims arising from the District's remote activation of webcams on student laptops.[5] Their proposed complaint seeks only equitable relief, including an order prohibiting LMSD from remotely activating webcams on student laptops, prohibiting LMSD from using laptop tracking technology that can compromise students' and families' privacy, and requiring LMSD to create and implement policies and practices for the District's administration of student laptops.[6]

On April 5, 2010, an HHS student and his parents filed a motion to intervene in the Robbins case to pursue claims arising from the District's remote activation of webcams on

[4] Robbins Compl. ¶ 23, App. Tab 203. Based on these allegations, the Robbins Complaint seeks compensatory, punitive, and liquidated damages, as well as attorneys fees, and unspecified declaratory and injunctive relief for alleged violations of the Electronic Communications Privacy Act, the Computer Fraud and Abuse Act, the Stored Communications Act, the Civil Rights Act, and the Pennsylvania Wiretapping and Electronic Surveillance Act, and for the alleged invasion of privacy under Pennsylvania common law. *See* Robbins Complaint ¶¶ 27-77, App. Tab 203.

[5] Motion of Colleen and Kenneth Wortley, Frances and David McComb, and Christopher and Lorena Chambers for Intervention, filed March 18, 2010 in Robbins, et al. v. Lower Merion School District, et al., No. 10-665 (E.D. Pa.) ("Wortley Intervention Motion"), App. Tab 205.

[6] Proposed Complaint in Intervention, attached to Wortley Intervention Motion, at pp. 11-12, App. Tab 205.

student laptops.[7] Their proposed complaint seeks only equitable relief – namely, an injunction permanently prohibiting the District from remotely accessing laptops "in a manner that constitutes an unreasonable search of students and their families," and a declaration restricting the dissemination of images captured by TheftTrack.[8]

Both motions for intervention are pending.

2. Government Investigations

On February 22, 2010, the United States Department of Justice issued a press release in which the United States Attorney's Office and the Federal Bureau of Investigation announced that they "would be involved in the inquiry into allegations that the Lower Merion School District activated web cams on computers issued to students."[9] The release quoted United States Attorney Michael L. Levy as saying that "[the United States Attorney's Office] intend[s] to work as a team with the Federal Bureau of Investigation, the Montgomery County District Attorney's Office, the Montgomery County Detectives, and the Lower Merion Police Department to determine if any crimes were committed. The issues raised by these allegations are wide-ranging and involve the meeting of the new world of cyberspace with that of physical space. Our focus will only be on whether anyone committed any crimes."[10]

To our knowledge, the government investigations are ongoing.

[7] Emergency Motion of the Neill Family to Intervene and for a Protective Order, filed April 5, 2010 in Robbins, et al. v. Lower Merion School District, et al., No. 10-665 (E.D. Pa.) ("Neill Intervention Motion"), App. Tab 206.

[8] Proposed Complaint in Intervention, attached to Neill Intervention Motion as Exhibit A, at p. 16, App. Tab 206.

[9] Department of Justice Press Release, dated February 22, 2010, App. Tab 197.

[10] Department of Justice Press Release, dated February 22, 2010, App. Tab 197.

3. The District's Engagement of Ballard Spahr

On February 19, 2010, the Board appointed Henry E. Hockeimer, Jr., and his law firm, Ballard Spahr, as special counsel with respect to the matters arising from LMSD's use of TheftTrack for student laptops.[11] Mr. Hockeimer, a former Assistant United States Attorney, and the Ballard Spahr lawyers working on these matters are experienced in conducting internal investigations, defending civil litigation, and defending individuals and entities in federal and state criminal investigations.

Consistent with its authority granted by the Board, Ballard Spahr engaged L-3 as a computer forensic consultant to provide information security, electronic discovery, and general computer forensic consulting services in support of Ballard Spahr's work for LMSD, and to report on pertinent technical issues.[12] L-3's engagement team is experienced in identifying and mitigating security risks for federal, state, and local governmental authorities, including school districts, collecting and preserving electronic data in a forensically secure manner, and computer forensic analysis.

III. NATURE OF THE INVESTIGATION

Ballard Spahr's investigation spanned 10 weeks and included, among other things: the collection and review of approximately 500,000 pages of documents from LMSD and other sources; interviews of 9 LMSD Board members and 31 District employees; interviews of 2 members of the Lower Merion Police Department; a number of informal discussions with Superintendent McGinley, Director of Information Services George Frazier, and other LMSD

[11] The Board ratified the appointment at its meeting on March 8, 2010. *See* Minutes of Board Meeting of March 8, 2010, App. Tab 4.

[12] L-3 Report at p. 1, App. Tab 1. Certain information in addition to student-identifying information has been redacted from the L-3 Report for security reasons.

administrators and IS personnel concerning information potentially relevant to the investigation; frequent consultation with and receipt of a report from L-3 concerning technical issues within the scope of the investigation; and independent research concerning LANrev and other pertinent technical issues, privacy and information security issues, and pertinent legal issues.

A. Immediate Actions Taken by LMSD on February 18, 2010

Within hours after learning about the Robbins lawsuit on the morning of February 18, 2010, at the direction of Dr. McGinley, the IS Department ceased all then-ongoing LANrev tracking of school-issued laptops. In addition, as a precautionary measure, the District removed the permissions required to activate TheftTrack from the LANrev administrator accounts of the two District staff members who had those permissions: IS Coordinator Carol Cafiero and Network Technician Michael Perbix.[13] The District also took steps to ensure that all relevant documents would be preserved.[14] And on February 19, 2010, Dr. McGinley wrote in a letter to parents and guardians that he had directed the following actions:

[13] On February 24, 2010, as a precautionary measure in light of the investigation and their roles in the activation of TheftTrack, the District placed Ms. Cafiero and Mr. Perbix on administrative leave.

[14] On February 22, 2010, the District agreed to an order subsequently entered by the Court in the Robbins litigation pursuant to which the District agreed, among other things: (i) not to remotely capture webcam photographs or screenshots from student laptops during the pendency of the litigation; and (ii) to preserve all pertinent electronic data. *See* Stipulation and Order, entered February 23, 2010, in Robbins, et al. v. Lower Merion School District, et al., No. 10-665 (E.D. Pa.), App. Tab 204. The District also agreed not to disseminate any images captured by LANrev (other than any images captured from the laptops issued to Blake J. Robbins and his sister, which the District provided to the Robbinses' counsel in connection with the litigation) to anyone without prior approval of the Court. *See* Order, entered April 15, 2010, in Robbins. As of the date of this Report, the District is working with United States Chief Magistrate Judge Thomas J. Rueter and the plaintiffs and proposed intervenors to develop a process pursuant to which students and/or their families will be: (i) notified if the investigation has recovered any images captured by LANrev from those students' laptops; and (ii) provided an opportunity to view any such images.

> - Immediate disabling of the security-tracking program.
>
> - A thorough review of the existing policies for student laptop use.
>
> - A review of security procedures to help safeguard the protection of privacy, including a review of the instances in which the security software was activated. We want to ensure that any affected students and families are made aware of the outcome of laptop recovery investigations.
>
> - A review of any other technology areas in which the intersection of privacy and security may come into play.[15]

B. Document and Data Collection and Review

Throughout our investigation, we requested that the District provide us with hard copy and electronic documents for the period from January 2007 through February 2010 concerning a wide range of subjects potentially relevant to the investigation. Among the broad categories of documents and data sought and obtained from the District were:

- Documents concerning the planning, implementation, and administration of the District's One-to-One laptop program;

- Documents concerning the District's decision to purchase the LANrev computer systems management software;

- Documents and data concerning the District's use of the TheftTrack feature of the LANrev software, including records of activations of TheftTrack, the reasons for activations, and any images resulting from those activations; and

- Documents concerning IS Department policies and procedures.

[15] Letter from C. McGinley to Parents and Guardians, dated February 19, 2010, App. Tab 27.

Using forensically secure means, L-3 collected and preserved electronic documents and data from, among other computing assets, the two dedicated LANrev servers, LMSD e-mail and file servers, the desktop and laptop computers used by District personnel believed to have documents or data potentially relevant to the investigation, and three laptops that had been used as "loaner" laptops for the One-to-One program. In addition, L-3 powered down and took physical custody of the LANrev servers. These steps are documented in detail in L-3's report of its forensic analysis, which is included in the Appendix to this Report at Tab 1. L-3 collected a total of approximately 19 terabytes of electronic data.

We received the full cooperation of the District and are satisfied that the District made available to us and L-3 all of the documents and data that we and L-3 requested.

C. **Interviews**

Beginning on the day after we were engaged – Saturday, February 20, 2010 – we met or spoke on several occasions with Dr. McGinley and Mr. Frazier to learn about the District's IS Department and relevant technology and personnel. Later, we and representatives of L-3 met with Mr. Frazier and other members of the IS Department for further background for our investigation. We also spoke informally with a number of teachers and other District employees about pertinent information or to request documents.

We formally interviewed 42 witnesses whom we believed may have had pertinent information. The witnesses interviewed included:

- Each of the nine members of LMSD's Board:
    - David Ebby, President
    - Linda Doucette-Ashman, Vice President
    - Diane DiBonaventuro
    - Gary Friedlander

    - Melissa Gilbert
    - Susan Guthrie
    - Lyn Kugel
    - Jerry Novick
    - Lisa Fair Pliskin
- Dr. Christopher W. McGinley (Superintendent)[16]
- Mike Kelly (Assistant Superintendent)
- Steve Barbato (Director, Curriculum Services)
- Scott Shafer (Business Manager)
- Jason Hilt (Supervisor of Instructional Technology)
- Dennis Witt (Supervisor, Custodians, Safety, and Security)
- Each of the nine principals and assistant principals at HHS and LMHS:
    - Steve Kline (HHS Principal)
    - Sean Hughes (LMHS Principal)
    - Doug Arnold (LMHS 12th Grade Assistant Principal)
    - Marcy Hockfield (LMHS 9th Grade Assistant Principal)
    - Scott Kilpatrick (LMHS 11th Grade Assistant Principal)
    - Lauren Marcuson (HHS Assistant Principal)
    - Wagner Marseille (LMHS 10th Grade Assistant Principal)
    - Philip Matilla (HHS Assistant Principal)
    - Lindy Matsko (HHS Assistant Principal)
- Ten Members of LMSD's IS Department

[16] Dr. Jamie Savedoff, who retired as LMSD's Superintendent in February 2008, declined our request for an interview.

  - George Frazier (Director, Information Services)[17]
  - Carol Cafiero (Information Systems Coordinator)
  - Brad Miller (Network Technician)
  - Michael Perbix (Network Technician)
  - Jeremy Valentine (Network Technician)
  - David Feight (Building-Level Technician, LMHS)
  - Kyle O'Brien (Building-Level Technician, HHS)
  - Chuck Ginter (Desktop Technician, HHS and LMHS)
  - Amanda Wuest (Desktop Technician, HHS)
  - Sherry Zielke (Secretary - Technology)

- Three LMSD Teachers:
  - Beth Hampton (Technology Integration Teacher, LMHS)
  - Christine Jawork (Social Studies Teacher, HHS)
  - Rhonda Keefer (Teacher on Special Assignment – Classrooms for the Future, HHS)

- Three Other LMSD Employees
  - Mike McGinley (Head Campus Aide, LMHS)
  - Debbie Williams (Bookkeeper)
  - Peg Flynn (Secretary to Assistant Principal, HHS)

- Two Lower Merion Police Department Detectives:
  - Detective Charles Craig
  - Detective Michael Flasinski

[17] Virginia DiMedio, who served as LMSD's Director of Technology for a number of years until June 2009, declined to be interviewed unless the District reimbursed her for the cost of engaging her own personal counsel in connection with her interview; the District declined to do so.

The interviews of Board members were conducted in person at LMSD's administrative offices or the offices of Ballard Spahr. The interviews of LMSD administrators and other employees were conducted in person at LMSD's administrative offices or at HHS. The interviews of the Lower Merion detectives were conducted in person at the Lower Merion Police Department headquarters. The topics covered included all of the issues that we address in this Report, as well as a number of background issues.[18]

In addition to our interviews, we reviewed the deposition testimony given in the Robbins litigation by Ms. Cafiero, Ms. Matsko, Mr. Perbix, and Mr. O'Brien. We also have considered questions raised by LMSD constituents and counsel for plaintiffs and the proposed intervenors in the Robbins litigation.

D. Independent Research

In addition to our review of documents and data from LMSD, we independently reviewed publicly available information concerning, among other things, the Pennsylvania Classrooms for the Future initiative, LANrev, computer tracking technology, and the community's knowledge of the issues we investigated. We also reviewed documents produced in the Robbins litigation by Absolute Software Corporation ("Absolute Software"), which acquired to rights to LANrev from Pole Position Software GmbH ("Pole Position") in December 2009.[19] And, we regularly drew upon the technical expertise of the L-3 engagement team.

[18] We did not interview any LMSD students. An order of the court in the Robbins litigation prohibits the District and its agents and representatives from contacting any member of the putative class, which includes students, about any of the issues raised by the litigation. Stipulation and Order, entered February 23, 2010, in Robbins, et al. v. Lower Merion School District, et al., No. 10-665 (E.D. Pa.), App. Tab 204.

[19] *See* Absolute Software Press Release, dated December 3, 2009, App. Tab 195.

IV. FINDINGS

A. LANrev Background

1. The District's Purchase of LANrev in Mid-2007

Even before the District launched the One-to-One program in the 2008-2009 school year, it had several thousand computers (both Macintoshes ("Macs") and Windows-based PCs) that were located at its various school campuses and administration buildings and issued to District personnel. At that time, student computer access was limited to computer labs and laptops that were stored on carts for classroom use. The IS Department had no centralized or automated way to manage those systems without handling each computer individually. Thus, installing new software, providing software updates and patches, and keeping track of system configurations was tedious and time-consuming.

In the Spring of 2007, under the direction of then-Director of IS Virginia DiMedio, the IS Department began searching for a systems management application that would allow it to automate and perform many of these administrative tasks remotely. IS Coordinator Carol Cafiero and Network Technician Mike Perbix considered potential alternatives, including LANDesk and LANrev, that could manage both Macs and PCs. Based on Internet reviews and advice from other network administrators with whom Mr. Perbix communicated through an on-line mailing list, they decided to test LANrev.

In May 2007, the District purchased 50 trial licenses of LANrev from Pole Position.[20] Mr. Perbix used the trial licenses to test LANrev on Macs and PCs in an LMSD lab and was pleased with the results, which he shared with Ms. Cafiero. Ms. Cafiero thus drafted a

[20] *See* LMSD Purchase Order No. 414631, dated May 9, 2007, App. Tab 13; E-mail from P. Byrd to M. Perbix, dated April 27, 2007, App. Tab 28. The 50 trial licenses cost $2,415.

memorandum to Ms. DiMedio in which she proposed that the District purchase 6,500 LANrev licenses to manage the computers on its network.[21] Ms. Cafiero wrote that LANrev "will enable us to manage both Mac and Windows computers on our network much more efficiently than we currently do," and as set forth below, she enumerated several features that made LANrev an attractive solution:

> Easier and faster software deployment. This is very important because laptops are "sleeping" when they are in their carts and cannot be managed unless they are outside of the cart and have a connection to the network. Currently when software needs to be installed, building Technicians must remove all of the laptops from a cart, install the software and then replace the computers back into the cart. That process is extremely inefficient when there are hundreds or even thousands of computers that need to have software installed. LANrev would allow us to use a central server to schedule the software installations and the laptops would automatically receive any software updates that are scheduled for them without the need for a technician to "touch" each computer.
>
> Cross Platform. The software works on both Mac and Windows computers and so does the management software. For administrative use, Windows clients can control Mac clients and Mac clients can control Windows clients.
>
> **Theft recovery feature. If a computer is stolen we can mark it stolen on the LANrev server and then the laptop will take screen shots and pictures of the user with the built-in camera and transmit that information back to our server along with information about the user's internet connection. That information can then be given to the authorities**. [Emphasis added.]
>
> Full hardware and software inventory. Information for each computer is gathered and stored on the LANrev server in a database that

[21] *See* E-mail from C. Cafiero to V. DiMedio, dated September 26, 2007, App. Tab 31.

> allows us to pull useful reports, such as a report that shows the age of each computer. That would be helpful when planning for replacement computer purchases.
>
> Easy initial deployment of the LANrev software. We don't even have to manually install the LANrev software on each computer. The LANrev server can scan the network for computers that do not have the LANrev client installed, and then install the LANrev client software automatically on those computers.
>
> Works with our existing software packages. Software packages that we currently install manually will work as-is without having to rebuild the packages.
>
> Increased functionality over Apple Remote Desktop. Apple Remote Desktop does not offer offline inventory or automatic software deployment.
>
> Will be an invaluable tool with 1-1. We can easily control which computers get certain software and simply schedule the software to be installed automatically as soon as the computer is connected to the network.[22]

Thus, according to Ms. Cafiero's memorandum, LANrev's TheftTrack feature – which is discussed in greater detail in the next section of this Report – was one of a number of features that led her and Mr. Perbix to advocate the purchase of LANrev. We did not find evidence suggesting that TheftTrack drove the District's decision to purchase LANrev. It is noteworthy, however, that during the trial period, Mr. Perbix showed a concern about potential abuse of TheftTrack's capabilities by asking Pole Position whether the District would be able to prevent TheftTrack from being used on – in the words of a Pole Position technical support

[22] E-mail from C. Cafiero to V. DiMedio, dated September 26, 2007, App. Tab 31.

person – “sensitive machines with confidential data such as finance and HR computers.”[23] A Pole Position technical support staff person initially explained that the only way to ensure that a certain computer is not tracked is for the administrator not to activate tracking for that computer, but Pole Position soon thereafter created a feature that would allow the District to exempt particular machines from tracking.[24]

In addition, Pole Position touted TheftTrack in its promotional materials, including a “case study” of the use of TheftTrack by the Bensalem (PA) Township School District to recover two MacBooks, one of which had been stolen from a student and the other of which was stolen from a teacher.[25] Noting that the Bensalem district had chosen LANrev in part for its ability to manage both Mac and Windows computers, Pole Position stated that the stolen laptops had returned 500 webcam photographs and other tracking data that the Bensalem and Camden, New Jersey police departments used to obtain search warrants. The article quotes a Bensalem district network technician as saying: “The police were amazed at the detailed tracking info provided by LANrev. Thanks to TheftTrack, our stolen MacBooks were recovered, the culprits apprehended, and we got the last laugh.”[26]

[23] *See* Pole Position technical support service ticket, created April 28, 2007 and updated June 7, 2007, App. Tab 30; *see also* E-mails between M. Perbix and B. Tran, dated April 27, 2010, App. Tab 29.

[24] *See* Pole Position technical support service ticket, created April 28, 2007 and updated June 7, 2007, App. Tab 30; *see also* E-mails between M. Perbix and B. Tran, dated April 27, 2010, App. Tab 29.

[25] *See* “Case Study: LANrev TheftTrack: Optimizing Recovery of Stolen Computers,” dated 2008, App. Tab 193.

[26] *See* “Case Study: LANrev TheftTrack: Optimizing Recovery of Stolen Computers,” dated 2008, App. Tab 193 (also discussing a Canadian school district’s use of TheftTrack to recover stolen computing assets). *See also* “LANrev Client Management: Adaptable, Comprehensive Management of All of Your Desktops,” dated 2008 (noting that “[a]rmed

(continued...)

In any event, after receiving Ms. Cafiero's proposal, Ms. DiMedio inquired whether Ms. Cafiero had reviewed the LANrev software with the other members of the IS Department, stating that she wanted a "consensus on this."[27] Ms. Cafiero responded that she and Mr. Perbix "love[d] LANrev," that Desktop Technician Amanda Wuest had seen a demonstration of the product, and that she would arrange for another demonstration for Network Technicians Brad Miller and Jeremy Valentine.[28] Ms. DiMedio then approved the purchase. On October 4, 2007, the District purchased 6,500 LANrev licenses for $143,975.[29]

2. How LANrev Works

As installed at LMSD, LANrev operated from two servers: the software server, which stored software and connected to managed laptops to install the software, and the inventory server, which received specification data from the managed laptops. LANrev could

(...continued)

with [the] information [that TheftTrack can capture], law enforcement should have little trouble recovering [a stolen] laptop"), App. Tab 194.

[27] E-mails between Ms. DiMedio and Ms. Cafiero, dated Sept. 26 & 27, 2007, App. Tab 32.

[28] E-mails between Ms. DiMedio and Ms. Cafiero, dated Sept. 26 & 27, 2007, App. Tab 32.

[29] *See* LMSD Purchase Order No. 314146, dated October 4, 2007, App. Tab 15. Under the Pennsylvania School Code, *see* 24 P.S. §§ 6-609, 6-610, "sole source" purchases (*i.e.*, of products available from only one source) are not subject to a public bidding process. Pole Position provided the District with a letter stating that it was the sole source of LANrev. *See* Letter from P. Byrd to C. Cafiero, dated December 7, 2007, App. Tab 33.

The Facilities/Purchasing Committee of the Board, which reviews District purchases that are within budgetary limits and thus within the discretion of the Business Manager, *see* LMSD Policy No. 610, Purchasing, App. Tab 10, reviewed the purchase of LANrev as part of a list of recent purchases at its meeting of June 15, 2007, and the Board ratified the purchase, among others, at its meeting of June 18, 2007. *See* List of Bills for Approval and Payment, dated June 18, 2007, at line 13, App. Tab 14; Minutes of Board Meeting of June 18, 2007, App. Tab 14. There is no evidence that the LANrev purchase was discussed at either the Facilities/Purchasing Committee or full Board meetings.

manage computers on which the LANrev "agent" software was installed.[30] Administering LANrev required the administrator software;[31] members of the IS staff who had LANrev administrator permissions thus needed the administrator software to be installed on their computers. By default, each client – if it was powered on and connected to the Internet – checked in with the inventory server every 15 minutes. This is how LANrev collected inventory information from the managed computers remotely. At each of these "heartbeats," the server determined, for example, whether the laptop was due for any software updates.[32] The interval between heartbeats could be reduced to as little as one minute.[33]

3. How TheftTrack Works

Although 18 members of the IS staff had certain LANrev administrator permissions at certain times during the 2008-2009 and 2009-2010 school years, and 16 of them at certain times during that period had access to relevant data stored on the LANrev server,[34] only Ms. Cafiero and Mr. Perbix had the heightened privileges required to activate or deactivate TheftTrack.[35] To activate TheftTrack for a particular computer, either Mr. Cafiero or Mr. Perbix

[30] LANrev User Guide Mac OS X Admin. Version, at 6, App. Tab 202.

[31] LANrev User Guide Mac OS X Admin Version, at 10, 13, App. Tab 202.

[32] LANrev User Guide Mac OS X Admin Version, at 51-52, App. Tab 202.

[33] *See* L-3 Report at 9.

[34] LMSD's network technicians, building-level technicians, and desktop technicians, and Supervisor of Instructional Technology Jason Hilt, had LANrev administrator privileges. *See* L-3 Report at 10-14.

[35] In an October 20, 2009 e-mail in which HHS Building-Level Technician Kyle O'Brien asked Mr. Perbix to activate tracking for a student laptop, Mr. O'Brien also asked if there was "[a]ny chance [Mr. Perbix] could just give [Mr. O'Brien] the ability to do this." App. Tab 60. Mr. Perbix responded: "Unfortunately, we can't give anyone else the ability to turn that on and off. Only Carol and I have the ability, and even though I know
(continued...)

had to select that particular laptop's agent name (*i.e.*, a unique code assigned to each District computer) from a list in the LANrev administrator application and manually choose to activate one or more of the following tracking options:

> (i) IP address (a numeric sequence identifying the network to which the computer is connected);
>
> (ii) screenshot; and
>
> (iii) webcam photograph.

When tracking was activated for a particular computer, at each heartbeat – if the computer was powered on, "awake," and connected to the Internet – it would send to the LANrev inventory server whichever information was selected: its IP address, a screenshot, and/or a webcam photograph. That data was stored on the LANrev inventory server until it was purged by a LANrev administrator. Deactivating TheftTrack likewise required selecting the particular computer from a list and choosing the appropriate options.

TheftTrack had no ability to capture video or audio. And, TheftTrack did not permit an administrator to take a photograph from any computer's webcam or capture a screenshot from any computer at any given moment on command; such images could be captured only through the automated process that was triggered when Ms. Cafiero or Mr. Perbix activated TheftTrack.[36]

(...continued)

it is a pain to email me etc etc, for your protection, you don't want to be able to turn that on and off…" [ellipsis in original]. E-mail from M. Perbix to K. O'Brien, dated October 20, 2009, App. Tab 61.

[36] Based on the available forensic data and other evidence, Ms. Cafiero activated TheftTrack 3 times on student laptops and Mr. Perbix activated it 161 times on student laptops. As set forth in Section IV(G) of this Report, there were 13 activations on student laptops for which we and L-3 were unable to determine who activated TheftTrack.

B. <u>One-to-One Laptop Initiative Background</u>

1. History and Rollout

As the Director of Technology and a member of the superintendent's cabinet,[37] Ms. DiMedio led the District's efforts to "infuse technology into the high school curriculum" through the receipt of grants under the Pennsylvania Department of Education's Classrooms for the Future ("CFF") initiative.[38] The CFF initiative was intended to increase the number of computers available for high school students' use, improve teachers' access to technology, and facilitate the professional development of teachers to promote competent and successful use of technology.[39]

In the 2006-2007 school year (the first year of the CFF initiative), LMSD received a grant of $415,024, and in the 2007-2008 school year it received $299,188.[40] LMSD used these grants to buy 300 laptops for classroom use and to create "Smart Classrooms."

As Dr. Savedoff and Ms. DiMedio wrote to District parents and guardians in June 2008, the District's One-to-One initiative – pursuant to which each high school student would be issued a laptop for use throughout the school year – grew out of efforts to enhance students' access to technology. They explained that funding for the One-to-One initiative was drawn from

[37] The cabinet is comprised of: the Assistant Superintendent, the Director of Human Resources, the Director of Operations, the Director of IS, and the Business Manager.

[38] LMSD Classrooms for the Future grant applications for program years 2006-2007 and 2007-2008, App. Tabs 17 and 19.

[39] *See generally* Pennsylvania Department of Education Classrooms for the Future Overview: Background, Purposes and Outcomes website, last visited April 29, 2010, App. Tab 21.

[40] *See* CFF Grant Applications for 2006-2007 and 2007-2008, App. Tabs 17 and 19, and Expenditure Reports for 2006-2007 and 2007-2008 school years, App. Tabs 18 and 20.

$721,000 in CFF grants and local funding.[41] Although the District initially intended to launch the program at HHS and LMHS in the 2008-2009 school year, logistical issues – including new high school construction – delayed implementation of the program at LMHS until the 2009-2010 school year. Accordingly, the District issued approximately 792 MacBook laptops to HHS students in September 2008, and approximately 2,306 MacBook laptops to HHS and LMHS students in September 2009. The LANrev agent software was included in the software package that LMSD installed on each of those computers. As a general matter, students were permitted to take their One-to-One laptops off campus. (Section IV(B)(2) of this Report addresses the District's failure to implement or follow consistent policies with respect to One-to-One laptops.)

2. One-to-One Laptop Guidelines and Policies

In July 2008, the District sent a letter from Ms. DiMedio to HHS parents and guardians outlining "Guidelines for Use of Student Laptops" and discussing the District's policy regarding insurance fees for One-to-One laptops.[42] (A similar letter was sent to HHS and LMHS students in July 2009.[43]) Among other things, the letter stated that:

> The laptop computers that will be issued to all Harriton students are the property of the Lower

[41] Letter from J. Savedoff and V. DiMedio to LMSD Parents and Guardians, dated June 6, 2008, App. Tab 22. Our understanding is that the laptops that had been purchased for high school classroom use with CFF grant funds were repurposed for use in LMSD elementary schools, thus eliminating a budgeted item for 2008-2009, and that the District purchased the One-to-One laptops from Apple at a discounted "CFF" rate negotiated by the Pennsylvania Department of Education. The District spent $1,237,858.84 for 2008-2009 and $2,382,659.80 for 2009-2010 on One-to-One laptops.

[42] Letter from V. DiMedio to HHS Parents and Guardians, dated July 25, 2008, App. Tab 23.

[43] *See* Letter from S. Kline to HHS Parents and Guardians, dated July 22, 2009, App. Tab 25; Letter from S. Hughes to LMHS Parents and Guardians, dated July 22, 2009, App. Tab 26.

> Merion School District. Students are responsible for the appropriate use of those laptops both at school and at home. The laptops are for the use of students for educational purposes. All commercial, illegal, unethical and inappropriate use of these laptops is expressly prohibited.[44]

The letter further stated that "[s]tudents should refer to the Student Acceptable Use Policy and their Guidelines [*sic*]."[45] Although not set forth in the July letter, students and parents or guardians were required to have signed previously, or to sign at the time of issuance of a One-to-One laptop, a document titled, "Acceptable Use Guidelines of the LMSD-NET by Students" ("Acceptable Use Guidelines"). The Acceptable Use Guidelines, which pertain to students' use of the District's computer network, were last revised no later than 2006, two years before the District launched the One-to-One initiative. They prohibit students from using the District's network for various inappropriate purposes, such as accessing obscene or pornographic materials and participating in chat rooms. They also state that in the event the District issues e-mail accounts to students, students "should know that email is not guaranteed to be private," and that the "Technology Coordinator has access to all mail."[46]

The Acceptable Use Guidelines were adopted pursuant to LMSD Policy No. 134, Acceptable Use of the LMSD-NET by Students ("Acceptable Use Policy"). The Acceptable Use Policy – which is posted on LMSD's website, but which to our knowledge was not directly distributed to students and parents or guardians in connection with the issuance of One-to-One

[44] Letter from V. DiMedio to HHS Parents and Guardians, dated July 25, 2008, App. Tab 23.

[45] Letter from V. DiMedio to HHS Parents and Guardians, dated July 25, 2008, App. Tab 23.

[46] Acceptable Use Guidelines of the LMSD-NET by Students, Lower Merion School District, App. Tab 12.

laptops – includes the general disclaimers that: (i) "the network administrator may review files and communications to maintain system integrity and ensure that students are using the system responsibly"; and (ii) "[u]sers should not expect that files stored on District resources will be private."[47]

In addition to setting forth usage guidelines, the July letters provided information about the District's policy with respect to insurance for One-to-One laptops. Families other than those who qualified for the free and reduced price lunch program were required to pay an annual insurance fee ($80 per student in 2008-2009 and $55 per student in 2009-2010), as well as a $100 deductible in the event of theft or damage. In both years, the July letters to parents and guardians stated that laptops for which insurance fees were not paid would not be permitted off campus, and that if such laptops were stolen or damaged while off campus, replacement or repair would be the responsibility of the student and parents.[48]

Neither the July 2008 and July 2009 letters to parents and guardians, nor the Acceptable Use Guidelines or the Acceptable Use Policy, however, disclosed the existence and capabilities of TheftTrack or addressed other privacy issues implicated by the issuance of laptops to high school students for their use on and off campus.[49]

[47] LMSD Policy No. 134, Acceptable Use of the LMSD-NET by Students, App. Tab 9. All official LMSD policies are posted on the District's website at http://www.lmsd.org/sections/about/default.php?t=board&p=board_policy&menu=board.

[48] *See* Letter from V. DiMedio to HHS Parents and Guardians, dated July 25, 2008, App. Tab 23; Letter from S. Kline to HHS Parents and Guardians, dated July 22, 2009, App. Tab 25.

[49] In an internal e-mail that preceded the July 2008 letter to parents and guardians, Ms. DiMedio set forth a number of One-to-One planning issues for HHS administrators and IS personnel. Although she included the security of on-campus storage sites as an issue for further consideration, she did not mention TheftTrack. E-mail from V. DiMedio to S. Kline, et al., dated July 8, 2008, App. Tab 39.

C. IS Department Personnel Withheld Information About the Capabilities and Their Use of TheftTrack from the Board, Administrators, and Students

In the months leading up to the Fall 2008 rollout of the One-to-One program, and continuing through 2009, the leaders and several members of the IS Department were not forthcoming with the Board, administrators, and students about what TheftTrack could do and how they used it. Each of the following incidents demonstrates an unwillingness on the part of IS personnel to let anyone outside of the IS Department know about TheftTrack's capabilities.

- January 14, 2008 Board presentation: On January 14, 2008, Ms. DiMedio and other members of the IS staff made an 87-minute presentation at the Board's Education Meeting titled, "Technology: A Look Back & Ahead to Classrooms for the Future."[50] They discussed the District's increasing use of technology, including classroom laptops. No one mentioned TheftTrack or the Department's ability to track computers generally.

- Spring 2008 presentations to the Board's Curriculum Committee: Ms. DiMedio made several presentations to the Curriculum Committee about the One-to-One program prior to its rollout.[51] Lyn Kugel, then-Chair of the Committee, followed up with several written questions for Ms. DiMedio, including:

  > Will all students be required to take the laptops home everyday after school, or will there be a storage area for students to drop off and pick up in the morning? What security features and personnel commitments would be associated with that? What are back-up plans for students who forget to bring their draft laptops to school?

[50] Video of the presentation is available on the District's website at: http://www.lmsd.org/sections/about/default.php?t=board&p=board_meetings_view&menu=board&vid=LMSB_080114_VP6_256K. An index of videos of Board meetings is at: http://www.lmsd.org/sections/about/default.php?t=board&p=board_meetings&menu=board.

[51] *See* Minutes of Meetings of the Curriculum Committee of March 21, 2008, April 23, 2008, and May 28, 2008, App. Tabs 5, 6, and 8.

> Please address security issues, annual update process, storage for computers and files.[52]

In her written response to the security questions, Ms. DiMedio did not mention the District's ability to track computers:

> There will be carts (that are currently in use) that can be used for temporary security during the day as well as recharging (during gym, for example). Student laptops will be collected over the summer for reimaging and maintenance, replacement, etc. We are currently investigating a number of file storage options in addition to server storage presently available. When students have their own laptops, they will be able to store project work on their own hard drive and burn their own back-up CDs or DVDs.[53]

- <u>Consultation with the District solicitor prior to the One-to-One rollout</u>: On May 14, 2008, an Apple employee suggested in an e-mail to Ms. DiMedio that she should discuss with the District solicitor "guidelines for Internet connectivity with school district owned computers when they are taken home":

  > You will need to ensure that your . . . policy covers the issue and also makes it clear that content placed onto the hard drive is the property of the district and can be examined by district personnel. You just want to be clear on where your responsibility begins and ends with regard to Internet access at home.[54]

  In a newspaper article published on May 2, 2010, Ms. DiMedio was reported to have said that on more than one occasion during the 2008-2009 school year she asked to meet with the solicitor to, in the reporter's words, "discuss the potential legal pitfalls of giving every student a laptop to take home" because there was no model for the District to follow, but that her requests were ignored. There is evidence, however, that at least one such meeting or discussion did occur. But we have found no evidence that Ms. DiMedio or any other District personnel

[52] E-mail from L. Kugel to V. DiMedio, et al., dated April 18, 2008, App. Tab 35.

[53] Presentation to the Curriculum Committee, "Creating a 21st Century Learning Environment," dated April 23, 2008, App. Tab 7.

[54] E-mail from B. Frey to V. DiMedio, dated May 14, 2008, App. Tab 37.

specifically advised the solicitor of the existence of TheftTrack, or sought advice from the solicitor concerning its use.[55]

- May 2008 e-mails between Mr. Perbix and LMHS Assistant Principal Wagner Marseille: On May 28, 2008, in an e-mail to Mr. Perbix and LMHS Building-Level Technician Dave Feight, Mr. Marseille wrote that he was investigating a missing laptop and asked to be "walk[ed] through the LoJack[56] system we have installed on our laptops." Mr. Perbix responded, and referring to TheftTrack, wrote only that: "One feature allows us to 'track' a computer when reported stolen. When a computer is being tracked, it reports back the IP and DNS info on where it is (meaning home network info etc) every 15 minutes or so. We can give that info to the police who can get a warrant to inquire to the internet service provider as to the account that holds that information." Mr. Perbix said nothing about TheftTrack's ability to capture images.[57]

- June 6, 2008 letter from Dr. Savedoff and Ms. DiMedio to parents and guardians: In their letter announcing the One-to-One initiative, Dr. Savedoff and Ms. DiMedio wrote that a "committee consisting of high school teachers and

[55] Apparently in light of the publication of the May 2, 2010 newspaper article, the District solicitor's office advised us on that day – the day before the date of this Report – that in the Summer of 2008 it drafted proposed laptop use agreements (for on-campus and off-campus use) and regulations concerning use of District-owned laptops. The draft agreements, which would have required signatures from students and parents or guardians, contained provisions advising students and their families that students should not have an expectation of privacy with respect to the computers or any files created, modified, stored, or otherwise accessed with the computers. The draft agreements did not address remote monitoring or webcam activation. As further discussed in Section IV(D)(2) of this Report, the drafts were provided to Assistant Superintendent Mike Kelly in August 2008. Neither the meeting with the solicitor nor the draft regulations and agreements arose in our interview of Mr. Kelly. And, as noted above (at p. 12, n. 17), Ms. DiMedio declined our request for interview (she is, however, expected to be deposed in the coming weeks in the Robbins litigation). In light of the foregoing, we intend to investigate these issues further and will report any additional findings to the Board as appropriate.

[56] LoJack Corporation is a provider of wireless tracking and recovery systems for mobile assets, particularly including vehicles. LoJack systems use covert radio frequency transmitters that, for example, enable police to track a stolen vehicle. *See* LoJack Corporation website, http://www.lojack.com/about/pages/about.aspx. As discussed elsewhere in this Report (at p. 36), some Board members and LMSD personnel had the mistaken impression that the District's computer tracking technology worked in a similar manner.

[57] E-mails between W. Marseille and M. Perbix, dated May 28, 2008, App. Tab 38.

administrators, technology personnel, parents, and students [had] developed a comprehensive plan to address the complexities of this project."[58] They did not address laptop security or student privacy, or disclose that the District would have the capable to activate the laptops' webcams or capture screenshots remotely.

- August 2008 e-mails regarding privacy concerns raised by a student intern: On August 11, 2008, shortly before the rollout of the One-to-One program at HHS, an HHS student who had been a student intern in the IS Department e-mailed Ms. DiMedio with the subject line "1:1 concern (Important)."[59] He wrote that he had recently learned of the District's purchase of LANrev and, describing his discovery of its ability to remotely manage computers while they are outside LMSD's network as "something startling," stated:

  > I would not find this a problem if students were informed that this was possible, for privacy's sake. However, what was appalling was that not only did the District not inform parents and students of this fact . . . .

  He further wrote:

  > [W]hile you may feel that you can say that this access will not be abused, I feel that this is not enough to ensure the integrity of students and that even if it was no one would have anyway of knowing (especially end users).
  >
  > I feel it would be best that students and parents are informed of this before they receive their computers.
  >
  > And while this only slightly sways my opinion on 1:1, i could see not informing parents and students of this fact causing a huge uproar.

  Ms. DiMedio responded seven minutes later:

  > I am not sure what you've found is correct. **What I do know for absolute certainty is that there is absolutely no way that the**

[58] Letter from J. Savedoff and V. DiMedio to LMSD Parents and Guardians, dated June 6, 2008, App. Tab 22.

[59] E-mail from Student Intern to V. DiMedio, dated August 11, 2008, App. Tab 40.

> **District Tech people are going to monitor students at home. There is no plan, no staff, no desire and I believe no technical way to do that.** I will definitely confirm the technical piece. If we are going to monitor student use at home, we would have stated so. Think about it—why would we do that? There is no purpose. We are not a police state. Lower Merion is one of the few school districts that only filters what we are required by federal law. **There is no way that I would approve or advocate for the monitoring of students at home.**
>
> I suggest you take a breath and relax.[60]

Ms. DiMedio then forwarded the e-mail chain to Mr. Perbix, who proposed a lengthy further response to the student intern that detailed LANrev's non-tracking features and described TheftTrack.[61] With Ms. DiMedio's approval,[62] Mr. Perbix sent an e-mail to the student intern that included the following:

> I will tell you that this feature is only used to track equipment that is reported as stolen or missing. The only information that this feature captures is IP and DNS info from the network it is connected to and occasional screen/camera shots of the computer being operated. This information is provided to police to hopefully assist in getting the laptop back to us. This feature has already been used to retrieve laptops that would have otherwise been lost and can only be activated by 2 people in the department. Once again, it is only used in the case where a laptop is reported as stolen or missing.
>
> The tracking feature does NOT do things like record web browsing, chatting, email or any other type of "spyware" features that you might be thinking of.

[60] E-mail from V. DiMedio to Student Intern, dated August 11, 2008, App. Tab 41 (emphasis added).

[61] E-mail from M. Perbix to V. DiMedio, dated August 11, 2008, App. Tab 41.

[62] E-mail from V. DiMedio to M. Perbix, dated August 11, 2008, App. Tab 41.

* * *

> Being a student intern with us means that you are privy to some things that others rarely get to see and some things that might even work against us.[63]

The student intern responded, thanking Mr. Perbix and stating that Mr. Perbix had "cleared up all [of his] concerns."[64] He also wrote:

> I assume you were referring to the conversation we had at the beginning of my internship here at Lower Merion and I want to reassure you that you should not think for a second that I would spread to people the "LoJack" like methods that the district employ[s].[65]

Continuing the e-mail conversation, Mr. Perbix wrote:

> [T]he "Big Brother" concern is a valid one. But, I assure you that we in no way shape or form employ any Big Brother tactics ESPECIALLY with computers off the network.[66]

- <u>November 3, 2008 presentation to the Board</u>: On November 3, 2008, Ms. DiMedio and Supervisor of Instructional Technology Jason Hilt gave a presentation to the Board titled, "Classrooms for the Future – Phase 1 Update (1:1)."[67] During the presentation, Board member Jerry Novick asked Ms. DiMedio about the District's experience with lost or stolen laptops. Ms. DiMedio said that LMSD had recently tracked and recovered six stolen laptops, but did not mention TheftTrack or describe the tracking technology:

  > We did have a theft and we have a way that we can track, and we did, and we got everything back. And all but, I think

[63] E-mail from M. Perbix to Student Intern, dated August 11, 2008, App. Tab 42.

[64] E-mail from Student Intern to M. Perbix, dated August 11, 2008, App. Tab 42.

[65] E-mail from Student Intern to M. Perbix, dated August 11, 2008, App. Tab 42.

[66] E-mail from M. Perbix to Student Intern, dated August 11, 2008, App. Tab 42.

[67] Mr. Hilt told us that Ms. DiMedio had told him that TheftTrack could be activated only with the involvement of the police. He said he realized that that was not true in the Summer of 2009 when he observed a photograph captured by TheftTrack.

> there were six that were taken, all but one came back in good shape, because we got it immediately. So, that's been the – the nice thing about this is when you have laptop carts and you're sharing, you have to wait until somebody notices that there's something missing. But as soon as those students found that their laptops weren't where they left them, they immediately reported them, we were immediately able to track them, so you don't have that lag time where you find out that the laptop was missing for a couple of months and nobody knew were it was. So, we're able to stay on top of the inventory much better with this.[68]

- Ms. DiMedio saw value in not publicizing TheftTrack's capabilities: Immediately following the filing of the Robbins lawsuit, Ms. DiMedio was quoted in a newspaper article as saying that "the district did not widely publicize the feature 'for obvious reasons. It involved computer security, and that is all it was being used for.'"[69] This attitude is consistent with accounts that we heard from several witnesses throughout our investigation. Ms. DiMedio reportedly declined to tell students about TheftTrack because doing so could "defeat its purpose."

- Mr. Frazier learned about TheftTrack soon after replacing Ms. DiMedio in the Summer of 2009 and recognized a need for a policy, but prioritized other projects: Although Mr. Frazier learned that the IS Department had computer tracking technology early in his tenure, he did not learn the full extent of TheftTrack's capabilities until Mr. Perbix advised him in late October 2009 about certain images that had been captured from a laptop issued to Blake J. Robbins.[70] In a November 2009 meeting with Ms. Cafiero, Mr. Perbix, and several LMSD high school principals and assistant principals, Mr. Frazier learned that the District had no formal policy governing the use of TheftTrack; as further set forth in Section IV(F) of this Report, the general practice was for a principal or assistant principal to request that TheftTrack be activated promptly upon determining that a

[68] Video of the November 3, 2008 Board meeting is available on the District's website at: http://www.lmsd.org/sections/about/default.php?t=board&p=board_meetings_view&menu=board&vid=LMSB_081103_VP6_256K. A transcript of the pertinent portion of the meeting is reproduced in the Appendix at Tab 3.

[69] Dan Hardy and Bonnie Clark, Student Claims School Spied On Him Via Computer Webcam, The Philadelphia Inquirer, February 19, 2010, App. Tab 196.

[70] *See* Section IV(G)(5), below.

> student's laptop was lost or missing. Mr. Frazier had reservations about TheftTrack and planned to raise the issue with the District's solicitor but over the next few months he was focused on issues that he considered more pressing – including network security vulnerabilities that he discovered early in his tenure – and did not raise the issue with anyone else.[71]

While the IS staff were guarded when discussing TheftTrack's capabilities with District constituents outside of the IS Department, they internally and otherwise expressed zeal for what TheftTrack could do.

In May 2008, Mr. Perbix participated along with a Pole Position employee in a webcast about LANrev.[72] The webcast was produced by MacEnterprise.org. According to its website, MacEnterprise.org, which is now known as MacEnterprise Inc., is a nonprofit organization that seeks to "provide a better service to the community in support of the Macintosh platform," and Mr. Perbix is a "director at large" of the organization.[73] Mr. Perbix gave a 40-minute presentation in which he said that he had selected LANrev for use at LMSD in light of its ability to manage both Mac and Windows computers. He also spoke at length about LANrev's inventory and remote management features. Speaking about TheftTrack, Mr. Perbix said that he

[71] In a recent newspaper article Ms. Cafiero was quoted as referring to this meeting and saying that Mr. Frazier opposed the use of TheftTrack but that the administrators favored it, and "the final decision was to keep doing what we were doing." John P. Martin, School Official Says Lower Merion Lacked Laptop Policy, Philadelphia Inquirer, April 30, 2010, at A1, App. Tab 200. We interviewed all of the known attendees of that meeting and none of them reported having had a conversation that pitted Mr. Frazier against the school administrators. Ms. DiMedio reportedly repeated this sentiment recently in another interview. A May 2, 2010 newspaper article states: "[Ms. DiMedio] believed that notifying everyone in the district of the tracking capability would defeat its purpose, effectively tipping off potential thieves." John P. Martin, Student Foresaw Web-Cam Troubles, Philadelphia Inquirer, May 2, 2010, at A1, App. Tab 201.

[72] *See* webcast description, available at http://www.macenterprise.org/webcasts/2008-archived-webcasts/lanrev46clientmanagement-may2008, last visited May 3, 2010.

[73] MacEnterprise Inc. website, http://www.macenterprise.org/about-us, last visited May 3, 2010.

"really really" liked the feature. He described how TheftTrack worked, and revealed that, "yes we have used it, and yes it has gleaned some results for us."[74] He also discussed having activated TheftTrack on a classroom laptop that was believed to have been stolen but quickly found; Mr. Perbix noted that by the time he deactivated TheftTrack, the program had captured 20 webcam images of a teacher and students using the laptop in class.[75]

Later in 2008, Mr. Perbix shared with the IS personnel the story of the District's successful use of TheftTrack – in consultation with the Lower Merion Police Department and the

[74] When it announced its acquisition of Pole Position, Absolute Software stated that "the technology, service, and support [for LANrev] will remain unchanged." *See* E-mail from P. Frankl to M. Perbix, dated December 3, 2009, App. Tab 195. Since the Robbins lawsuit was filed, however, Absolute Software has distanced itself from the TheftTrack feature. In March 29, 2010 testimony before the Senate Judiciary Committee Subcommittee on Crime and Drugs, Absolute Software CEO John Livingston said that Absolute Software had created a software patch to disable the webcam feature of TheftTrack. He also noted that Absolute Software's LoJack technology, in contrast to "user oriented solutions" like LANrev, relies on the company's "staff and highly trained former law enforcement personnel." Prepared Statement of John Livingston to the Senate Judiciary Committee Subcommittee on Crime and Drugs, dated March 29, 2010, App. Tab 198.

[75] In a June 2009 e-mail to a technician at another school, Mr. Perbix explained several methods for remotely monitoring networked computers. (Mr. Perbix frequently communicated with other IS professionals via e-mail groups and the like.) About LMSD's systems, he wrote:

> We use LANrev to monitor the equipment (not the users) and keep up with inventory and helpdesk type activities. . . .
>
> As far as the Theft Track feature, that is engaged only when a laptop is reported as missing. At that point, only 2 of us can engage the theft tacking which records IP and DNS information of the laptop, take a screen shot (if wanted) and takes a camera shot (if available and wanted).

E-mails between M. Perbix and P. Rothman, dated June 10, 2009, App. Tab 56.

Montgomery County District Attorney's Office – to recover a laptop that was stolen from the car of a Belmont Hills Elementary School teacher.

> I just thought I would share this story with everyone who did not know . . . .
>
> A teacher had a laptop stolen from her car off of school grounds. The laptop was reported stolen December of last year. At that time we were just starting to roll out LANrev to a test group of computers. We were lucky enough to get LANrev on that computer before it was stolen.
>
> After hearing about it I activated the Theft Tracking feature. It was another month until the computer started reporting in and we were obtaining IP Addresses, DNS and pictures. We notified the police and they went to the house belonging to the IP address, but the occupants did not match the description of the people in the picture.
>
> Months later, the laptop again appeared, but this time it was reporting with an IP address and DNS from PAKISTAN. After several months, the laptop reported back from the same area as originally reported. This time the police went to the house being reported and RETRIEVED the laptop. The house they went to on the first instance was THE NEIGHBOR who must have had an open wireless network.
>
> So . . . after a year, we have our laptop back.
>
> Just a good story to share amongst all the issues we deal with day to day.
>
> Thank you Jeremy for staying on the police to get this recovered.[76]

As set forth in Section IV(G)(9)(a) of this Report, the laptop tracked to Pakistan was the source of 5,323 images (2,706 webcam photographs and 2,617 screenshots) recovered in our

[76] E-mail from M. Perbix to LMSD Technology Group, dated December 5, 2008, App. Tab 53.

investigation. We learned that Mr. Perbix and other members of the IS Department enjoyed telling the story of the "Pakistan" laptop.

In the wake of another theft incident – in which six laptops were stolen from an HHS locker room in September 2008 – several IS employees discussed by e-mail the use of both security camera footage and TheftTrack to try to recover the laptops. After Ms. Cafiero wrote that LANrev had captured images from one of the laptops, HHS Desktop Technician Amanda Wuest wrote, "This is awesome. It's like a little LMSD soap opera," and Ms. Cafiero replied, "I know, I love it!"[77]

And in September 2009, Mr. Perbix reacted negatively when Mr. Frazier told him that he had received a question about disabling a laptop webcam. After noting that only he and Ms. Cafiero "ha[d] access to operate the camera remotely," Mr. Perbix wrote:

> In my opinion, in the interest of theft protection, teachers should not even be allowed to cover the camera like they do now…if their laptop gets stolen, that is a major piece of the theft tracking gone bye bye just because someone is uninformed on what the use of the camera is.
>
> The camera can NOT be used without the little green light being on…so if it is on, they will know it. And as I said, only Carol and I have the ability to enable theft track which does not record video, only a snapshot every 15 minutes.
>
> Is someone afraid that we are spying on them?[78]

Nevertheless, enthusiasm among IS personnel for the TheftTrack technology was not untempered. For example, discussing whether the police and Dennis Witt, LMSD's

[77] E-mails among C. Cafiero, A. Wuest, et al., dated September 19, 2008, App. Tab 46.

[78] E-mails between M. Perbix and G. Frazier, dated September 11, 2009, App. Tab 58. Our investigation revealed no e-mail from Mr. Frazier responding to Mr. Perbix.

Supervisor of Custodians, Safety, and Security were taking the TheftTrack information from the "Pakistani" laptop seriously, Ms. Cafiero said that "it is not for us to play police for them." Mr. Perbix replied, "Shame to say, but I agree."[79] And in the context of a February 2009 discussion about whether to purchase Dell laptops without built-in webcams, Ms. Wuest wrote that it "[m]ay not be the worst idea for privacy issues to eliminate the webcam if someone makes the decision it isn't necessary."[80] We found no evidence that Ms. Wuest or others copied on her e-mail further explored the "privacy issues" to which Ms. Wuest referred.

D. To the Extent Certain Board Members or District and School Administrators Nevertheless Had Some Knowledge of the District's Ability To Track Laptops, They Did Not Seek Enough Further Information or Advice, or Sufficiently Voice Concerns They May Have Had

Notwithstanding that IS personnel did not openly discuss the webcam photograph and screenshot features of TheftTrack, there is evidence that certain Board members and administrators knew at least that the IS Department could somehow track laptops. Although some efforts were made to learn more information, those inquiries could have been pursued further.

1. Board Members' Knowledge of Computer Tracking

Several Board members believed that the student laptops had tracking technology akin to a LoJack system that would allow the police to track a signal emitted by the laptops. And at least one Board member believed that the tracking technology allowed the IS Department to capture a one-time webcam photograph of a stolen laptop when the laptop was opened.

[79] E-mails between M. Perbix and C. Cafiero, dated September 18, 2008, App. Tab 44.

[80] E-mails among A. Wuest, C. Cafiero, et al., dated February 23, 2009, App. Tab 54.

While there is no evidence that any Board members pressed the IS staff to learn more about the tracking technology, had or expressed any concerns that the District's tracking technology could threaten students' privacy, or sought advice from the District's solicitor about these issues, there also – as discussed in the previous section of this Report – is little evidence that IS personnel ever shared with the Board any meaningful information about the existence and use of their computer tracking capabilities that might have given rise to such questions or concerns. Notably, five of the nine Board members have children who attend LMSD high schools and have been issued One-to-One laptops.

2. District Administrators' Knowledge of Computer Tracking

Superintendent Christopher McGinley learned about TheftTrack at a Cabinet meeting in 2008 when he was told about the theft of several laptops from an HHS locker room.[81] He advised us that until the Robbins lawsuit was filed, his understanding was that TheftTrack: (i) was used only in conjunction with the police when the District had filed a police report for a missing laptop; and (ii) captured a single webcam photograph when the laptop was opened – not periodic webcam photographs and screenshots while TheftTrack was activated. He also said that he had no discussions about the need for a policy governing the use of TheftTrack before filing of the Robbins lawsuit. We found no evidence to the contrary.

Like Dr. McGinley, Assistant Superintendent Mike Kelly reported that his understanding was that TheftTrack captured a single webcam photograph when the laptop was opened. And, although he heard generally about laptops being stolen and recovered, he had not had specific discussions about the District's tracking capability. But, as discussed above (at p.

[81] Dr. McGinley told us that he did not recall the discussion of that incident at the November 3, 2008 Board meeting at which Ms. DiMedio said "we have a way that we can track" in response to a Board member's question. (*See* Section IV(C), above.)

27, n. 55), we learned on the day before the date of this Report that Mr. Kelly was provided by the District solicitor's office with draft laptop use agreements and regulations in August 2008, and that those drafts addressed student privacy issues, albeit not specifically in the context of remote monitoring. We have not yet learned what became of those drafts but will investigate that issue further and supplement our Report to the Board as appropriate.

3. High School Administrators' Knowledge of Computer Tracking

As a general matter, high school administrators (*i.e.*, principals and assistant principals) had a better sense of TheftTrack's capabilities than Board members and District-level administrators.

HHS Principal Steve Kline said that he learned about TheftTrack from an incident in which six laptops were stolen from an HHS locker room in September 2008. Shortly after the theft, Mr. Kline was copied on and responded to an e-mail in which members of the IS Department discussed tracking and obtaining images from the stolen computers.[82] A few weeks later, Mr. Kline received an unrelated e-mail from Jason Hilt, then the "teacher on special assignment" to the One-to-One program, explaining that "[w]e are currently tracking all uninsured laptops" and "there are 20+ uninsured laptops online off campus."[83] (Those computers were tracked via IP address only; not via webcam photographs or screenshots.) Mr. Kline forwarded the e-mail to HHS Assistant Principals Lauren Marcuson and Lindy Matsko for discussion at an upcoming meeting.[84] And in early November 2009, Mr. Kline met with Ms.

[82] E-mail from S. Kline to M. Perbix, et al., dated September 19, 2008, App. Tab. 45.

[83] E-mail from J. Hilt to S. Kline, dated October 2, 2008, App. Tab. 51.

[84] E-mail from S. Kline to L. Marcuson, et al., October 2, 2008, App. Tab 51.

Matsko about photos and screenshots taken from Blake J. Robbins's loaner laptop that Mr. Perbix had placed in their home directories.[85]

Mr. Kline reported that soon after he learned about TheftTrack in September 2008, he asked Ms. DiMedio whether LMSD should advise students and parents about it, and Ms. DiMedio responded "no" because, according to her, doing so would undermine TheftTrack's effectiveness. Mr. Kline never revisited the subject of formally advising students and parents about the existence of TheftTrack.

LMHS Principal Sean Hughes said that he learned about TheftTrack when a stolen teacher's laptop was tracked to Pakistan. Mr. Hughes said that he thought that many students heard about that incident. He also said that like Mr. Kline, he responded accurately when students asked him about the tracking feature, and that he encouraged LMHS teachers to do the same.

Certain assistant principals sometimes were involved in helping to recover missing laptops. As set forth below, they learned about at least some of TheftTrack's capabilities in that context.

- In May 2008, Ms. Marcuson submitted a Help Desk ticket stating that she understood that "some of the laptops at LMHS take a 'snapshot' of the student when they turn on the computer" and asked whether HHS computers had the feature because HHS had situations "where this will come in very handy." Desktop Technician Amanda Wuest responded that TheftTrack had "been rolled out in most of the computers in the district." [86]
- In September 2009, Mr. Perbix e-mailed Mr. Kline, Ms. Marcuson, and Ms. Matsko to ask whether they recognized the person in the attached webcam photograph. After asking Mr. Perbix to brighten the photograph, Ms. Marcuson

[85] E-mail from M. Perbix to S. Kline, dated October 30, 2009, App. Tab. 63.

[86] Help Desk ticket submitted by L. Marcuson, dated May 9, 2008, App. Tab. 36.

said that she did not recognize the person and suggested that the photograph be sent to the police.[87]

- LMHS Assistant Principals Doug Arnold, Marcy Hockfield, Scott Kilpatrick, and Wagner Marseille all said that they recalled hearing about the laptop that was tracked to Pakistan, but did not recall ever seeing an image captured by TheftTrack.[88]

- As further discussed in Section IV(G)(5) of this Report, Ms. Matsko viewed certain images that had been captured from a One-to-One loaner laptop issued to Blake J. Robbins.[89]

Although they had varying levels of knowledge about Theft Track and experience with its capabilities – and thus varying potential bases for concern about its use – we found no evidence (with the exception of the question Mr. Kline posed to Ms. DiMedio about alerting students and parents) that any of the HHS or LMHS principals or assistant principals raised with anyone any privacy concerns arising from the use of TheftTrack.

E. **<u>Certain Teachers and Students Knew or Had Suspicions About the District's Ability to Capture Webcam Photographs Remotely</u>**

Although we have no evidence that teachers or students fully understood how TheftTrack worked or how or to what extent the IS Department used it, we heard directly and anecdotally that certain teachers and students knew or had suspicions about the District's ability to capture webcam photographs remotely.

As discussed in Section IV(C), above, a former IS Department student intern raised with Ms. DiMedio and Mr. Perbix concerns that TheftTrack could threaten students'

[87] E-mails among M. Perbix, S. Kline, et al., dated September 7, 2009, App. Tab 57.

[88] As noted in Section IV(C) of this Report, Mr. Perbix described TheftTrack to Mr. Marseille without mentioning its image-capturing capabilities. Like Mr. Marseille, Ms. Hockfield also had understood the tracking feature to be a "LoJack"-like device.

[89] *See* E-mail from M. Perbix to L. Matsko, dated October 30, 2009, App. Tab. 63.

privacy. We have no evidence that Ms. DiMedio or Mr. Perbix shared the student's concerns with anyone else, or that the student raised his concerns with any administrators.

According to Mr. Kline, however, two HHS students informally approached him in January 2009 and asked whether the District had the ability to remotely capture webcam photographs from student laptops. Mr. Kline advised us that he responded that the District did have that ability and activated the technology only when laptops were reported stolen, as he believed was the case. Mr. Kline also reported that other students asked about the webcams from time to time and that he, and to his knowledge, his staff, always responded the same way.

We learned in our interviews that some students knew that remote webcam activation had assisted in recovering the stolen teacher's laptop that was tracked to Pakistan. Also, certain students and teachers also had suspicions about the webcams that arose because they either saw the green light next to the webcam on their laptops turn on momentarily or heard from others that the green lights on their laptops had turned on momentarily.[90] In response to those suspicions, we learned that some teachers covered the lenses of the webcams on their laptops. Christine Jawork, a ninth grade teacher at HHS, advised us that she had told students that the District could remotely activate their laptops' webcams as a means of tracking lost laptops, and that she had taped over the webcam on her laptop.[91] She also said that her students had discussed the green lights turning on.

[90] We also were told by several IS staff members that they saw or heard about a webcam photograph of a student who they believed to be intentionally "giving the finger" to the webcam.

[91] Jason Hilt, the Supervisor of Instructional Technology, also told us that he taped over his webcam in the 2009-2010 school year after he learned that TheftTrack could be activated without police involvement, and that he shared his concern about remote webcam activation with Mr. Frazier and Director of Curriculum Services Steve Barbato. Mr. Frazier shared Mr. Hilt's concern but gave other IS issues higher priority; Mr. Hilt

(continued...)

As set forth in the L-3 Report, the green light next to the webcam may activate when any program – such as iChat, an Apple instant messaging program that allows video chatting via webcams, or LANrev's TheftTrack feature – accesses the webcam. Thus, a green light was not necessarily indicative of LANrev capturing a photograph with the TheftTrack feature. In any event, there were 76 activations of TheftTrack on One-to-One laptops that involved image tracking in the 2008-2009 and 2009-2010 school year. Thus, to the extent that a One-to-One laptop's green light flashed for an unknown reason and the computer was not one of those that we have determined was tracked, it is highly unlikely the flashing green light was evidence that TheftTrack was activated for that computer.[92]

F. The District and the IS Department Failed to Adopt Official Policies or Procedures for the Use of TheftTrack

The District had no official policies or procedures for the use of TheftTrack. Neither the Board, District-level administrators, school-level administrators, nor even the leaders of the IS Department imposed any official restrictions on the use of LANrev's tracking features.

This policy void was characteristic of the IS Department over the last several years. Mr. Frazier described the department upon his hiring in July 2009 as the "Wild West" because there were few official policies and no manuals of procedures, and personnel were not evaluated regularly. Mr. Frazier reported, among other things, that IS staff routinely struggled

(...continued)

recalled that Mr. Frazier inherited "hundreds" of problematic issues in the IS Department. Mr. Barbato told us that he had heard from Ms. DiMedio that when activated, the tracking feature would take one webcam photograph when the laptop was opened. He also told us that he had assumed that students and parents knew about the tracking feature.

[92] The L-3 Report, at pp. 19-20, discusses the high degree of completeness of L-3's recovery of LANrev command data (for TheftTrack activations and the full range of other LANrev actions requiring a command).

with thorny issues for which they had no formal guidance, such as how to respond to reports that certain students were engaged in "sexting" using District computers. Mr. Frazier also immediately discovered a host of computer security vulnerabilities that he considered his highest priority in his first few months as Director of IS. For example, he found that LMSD's network was vulnerable to outside attacks and that network access passwords had not been changed for years, if ever. Technology and IS staffing issues related to the impending opening of the new HHS building also commanded much of Mr. Frazier's attention at the beginning of his tenure. Thus, although Mr. Frazier made a note to himself to follow up with the District's solicitor, Ken Roos, at a November 10, 2009 One-to-One meeting at which he discussed the lack of a laptop tracking policy, he did not do so.[93]

In any event, the lack of policies and procedures governing the use of TheftTrack was evident in January 2008 when a laptop was stolen from Belmont Hills Elementary School. Mr. Perbix reported to Ms. DiMedio and Ms. Cafiero that TheftTrack had collected IP address data, screenshots, and webcam photographs. Ms. DiMedio said that she was "sending this to the Cabinet for next steps," but Mr. Perbix said, "shouldn't this go to Dennis Witt and give the info [*sic*] to the police?"[94] As set discussed in Section IV(G)(9)(a), below, the District worked with the Lower Merion Police Department, which eventually recovered the laptop.

No procedure had been determined eight months later when, in the first month of the One-to-One program, six laptops were stolen from an HHS locker room. In that incident, TheftTrack worked as intended: it captured images of the suspects and the District provided the

[93] One-to-One Meeting Agenda, dated November 10, 2009, App. Tab 16.

[94] E-mails between M. Perbix, V. DiMedio, and C. Cafiero, dated January 15, 2008, App. Tab 34.

images to the Lower Merion Police Department, which apprehended the suspects and recovered the laptops.[95] The day after the theft, however, Ms. Cafiero e-mailed Ms. DiMedio seeking guidance regarding the procedures to be followed in such circumstances:

> Can we please get a procedure or some chain of command together next week? Everyone wants to help and that's great, but we need to be clear about who does what. Why did Dennis [Witt] call Mike [Perbix]? Maybe only supervisors should be dealing with this information. Right now we have half our department spending time and duplicating efforts. Mike has been out for 1.5 weeks and he has a lot of stuff to catch up on this week. I don't want him spending his time on this if it is something I can do.[96]

Ms. DiMedio responded:

> Sure. I don't know why he called Mike except that Mike has worked on this before. And, I don't know how Amanda got involved either. Someone must have called her. I think it is probably one of those things that take a life of its own. Most of the people have never been involved before and don't know what to do. We have so many procedures for so many incidents, they either don't know or forget. In any instance, they should notify a Supervisor. They should also contact Building Admin and Dennis Witt. Question is -- should it be email or phone or both. We'll get it together next week.[97]

Such policies, however, never came together. To the contrary, a number of administrators told us that they sought guidance from Ms. DiMedio about various administrative

[95] More details about these laptops are set forth in Section IV(G)(2) of this Report, below.

[96] E-mails between C. Cafiero and V. DiMedio, dated September 20, 2008, App. Tab 50.

[97] E-mails between V. DiMedio and C. Cafiero, dated September 20, 2008, App. Tab 50.

issues with the One-to-One program, but that it was not forthcoming.[98] Instead, they "flew by the seat of their pants." In the absence of official guidance, informal procedures for the activation of TheftTrack developed, but they changed over time and were not followed consistently.

As a general matter, with respect to laptops that were missing (*i.e.*, lost or stolen):

(i) the student reported a laptop missing to a school administrator (*i.e.*, an assistant principal or a principal);

(ii) the administrator worked with the student to determine whether the laptop was merely misplaced;

(iii) if the laptop was not located, the administrator notified a building-level technician of the missing laptop;

(iv) the technician notified either Ms. Cafiero or Mr. Perbix, requesting that she or he activate TheftTrack for the missing laptop;[99] and

(v) if the laptop was found or recovered, that fact was reported to Mr. Perbix or Ms. Cafiero, and Mr. Perbix or Ms. Cafiero deactivated tracking.

These procedures evolved over time and were not followed consistently. In addition, recordkeeping was informal and inconsistent.

[98] Ms. Cafiero was quoted in a recent newspaper article as saying that she revisited the subject at a meeting with Mr. Frazier in August 2009 and that no decision was made about policies at that meeting either. John P. Martin, School Official Says Lower Merion Lacked Laptop Policy, Philadelphia Inquirer, April 30, 2010, at A1, App. Tab 200. Other witnesses interviewed did not recall that discussion.

[99] In at least three instances of theft, the security supervisor, Dennis Witt, contacted the Lower Merion Police Department and Mr. Perbix exported from the LANrev server images that had been captured from the laptops and uploaded them to a secure, password-protected portion of the LMSD website that the police could access. *See e.g.*, E-mail from J. Valentine to Det. Craig, et al., dated September 23, 2008, App. Tab 49; E-mails between D. Witt and M. Perbix, dated June 10, 2009, App. Tab 49. The District also worked with the police with respect to at least three other laptop thefts without providing images obtained via TheftTrack.

Similar problems plagued the District's handling of One-to-One laptops for which insurance payments were not made. Pursuant to the policy provided to students and parents and guardians, such laptops were not permitted to be brought off campus. But responsibility for enforcing that policy was never clearly delegated to any department or individual. This created tension between administrators and IS personnel: as a general matter, administrators did not think that they should be responsible for collecting laptops or debts, and IS personnel did not think that they should be responsible for confiscating laptops.[100]

Mr. Hilt consulted with Mr. Perbix, who informed him that the IS Department could use IP address tracking to determine whether students were inappropriately taking their laptops off campus (an IP address other than that of LMSD's network would indicate that the student was using the computer elsewhere). For several months, Mr. Perbix tracked laptops for which insurance fees were unpaid using IP-only tracking (meaning that no images were captured

[100] This tension was not limited to the insurance issue. For example, in September 2008, upon being advised that a student had withdrawn from school and not returned his laptop, Ms. Cafiero wrote:

> I will turn on tracking for this computer. I do hope that the Harriton administrators aren't relying solely on us gathering up the location of the computer. Our computer tracking can only do so much. The Harriton administrators need to be calling the student's parents, etc. in an effort to get back the laptop.

Mr. O'Brien responded:

> Agreed. I am on my way to talk to Jason so we can come up with some type of procedure for this scenario. After we discuss we will let you and HH admin decide the best course of action.

E-mails among C. Cafiero, K. O'Brien, et al., dated September 16, 2008, App. Tab 43. These tensions surfaced again in March 2009 when Ms. Marcuson and Ms. Cafiero disagreed about whose responsibility it was to "police" laptops.

from the tracked laptops). Mr. Perbix explained how he was doing that in an October 2, 2008 e-mail on which he copied Ms. DiMedio.[101] He provided the results to Mr. Hilt,[102] who in turn contacted families to collect payment.[103] During the 2008-2009 school year, 67 laptops were tracked (via IP-only tracking) in light of unpaid insurance fees.

By March 2009, the high volume of tracking data began causing LANrev to run slowly. Working with Pole Position technical support staff,[104] Mr. Perbix determined that the problem was that IP-only address tracking on approximately 100 laptops had filled the database.[105] As further discussed in Section IV(I) of this Report, Mr. Perbix solved the LANrev performance problem by purging the database. Meanwhile, Mr. Hilt had concluded that using TheftTrack was an ineffective way of enforcing the insurance requirement. As a further reflection of the confusion and lack of communication about policies and procedures, Ms. DiMedio wrote, upon learning about the problem with the LANrev database:

> I said from the beginning that those who did not pay for insurance should leave the laptops in the building. If the laptop is lost or stolen off

[101] E-mail from M. Perbix to J. Hilt, et al., dated October 2, 2008, App. Tab 52.

[102] *See, e.g.*, E-mail from M. Perbix to J. Hilt, et al., dated October 2, 2008 (reporting at 7:24 p.m. that, based on the IP-only tracking results, two of the "no insurance" laptops had been brought to the students' homes), App. Tab 51.

[103] The same day, Mr. Hilt advised Mr. Kline that "[w]e are currently tracking all uninsured laptops" and that on that day as of 5:00 p.m., there were "20+ uninsured laptops online off campus." E-mail from J. Hilt to S. Kline, dated October 2, 2008, App. Tab 51.

[104] *See* E-mails among M. Perbix and Pole Position technical support staff, dated from March 6 through March 13, 2009, App. Tab 55. A Pole Position technical support person had advised Mr. Perbix in April 2007 "that TheftTrack does generate a good deal of data since information is sent in with each heartbeat," and could "quickly fill up your database," depending on the number of computers on which TheftTrack was activated at a given time. E-mail from B. Tran to M. Perbix, dated April 27, 2007, App. Tab 29.

[105] E-mails between M. Perbix and M. Bestmann, dated March 12, 2009, App. Tab 55.

> site, they are responsible. I never said to turn tracking on for them. I don't know who gave that instruction but it wasn't me.[106]

Particularly after March 2009, Mr. Perbix periodically asked the technicians who requested the activation or deactivation of TheftTrack whether TheftTrack should remain activated for laptops that were being tracked. These questions often resulted in deactivations because the laptops had been found.[107] Accordingly, Mr. Perbix's diligence prevented the further collection of images from laptops in the possession of students. But the ad hoc nature of these exchanges illustrates the serious policy deficiencies that gave rise to the unwarranted collection of thousands of images of students.

G. The District's Use of TheftTrack

Analysis of all of the available forensic data and other evidence collected during the investigation reveals that TheftTrack was activated 177 times on One-to-One program laptops during the 2008-2009 and 2009-2010 school years. Those activations can be grouped into seven general categories: (i) IP-only tracking; (ii) stolen laptops; (iii) laptops not returned by students who withdrew from school; (iv) missing laptops; (v) uninsured loaner laptop brought off-campus; (vi) mistaken activations; and (vii) reason for activation unknown. Each of the activations within those categories is detailed below.

In addition, analysis of all of the available forensic data and other evidence collected during the investigation reveals that TheftTrack was activated 25 times on laptops

[106] E-mail from V. DiMedio to C. Cafiero, dated March 12, 2009, App. Tab 111.

[107] *See, e.g.*, E-mails between M. Perbix and D. Feight, dated April 28, 2009, App. Tab 122; E-mails between M. Perbix and K. O'Brien, dated October 21, 2009, App. Tab 62; E-mails between M. Perbix and D. Feight, dated November 18, 2009, App. Tab 162; E-mails between M. Perbix and D. Feight, dated December 8, 2009, App. Tab 174; E-mails between M. Perbix and K. O'Brien, dated February 18, 2010, App. Tab 192.

designated for classrooms or unassigned loaner laptops and 12 times on laptops issued to teachers. Details about those activations also are set forth below.

1. IP-Only Tracking of Student Laptops

Between September 29, 2008 and September 21, 2009, IP-only tracking was activated on 101 student laptops: 67 laptops for which insurance was not paid; 26 student laptops that were not returned at the end of the school year;[108] and 8 laptops that were not permitted off campus in light of disciplinary sanctions.[109] None of these activations resulted in the capture of webcam photographs or screenshots.

Student[110]	Date On	Requested by	Activated by	Deactivated by	Date Off	Webcam Photos	Screen-shots	App. Tab[111]
27	Unknown	Hilt	Unknown	Perbix	3/12/09	0	0	112
32	Unknown	Hilt	Perbix	Perbix	3/12/09	0	0	112
79	Unknown	Hilt	Unknown	Perbix	3/12/09	0	0	112
98	Unknown	Hilt	Unknown	Perbix	3/12/09	0	0	112
6	9/29/08	Hilt	Perbix	Perbix	11/7/08	0	0	79-80

[108] On June 12, 2009, IP-only tracking was activated on 26 student laptops that were not returned at the end of the 2008-2009 school year. On June 17, 2009, Mr. Hilt sent a letter to the parents and guardians of the students who had not returned their laptops and advised them that the Lower Merion Police Department would be notified if the laptops were not returned by June 26, 2010. *See* Letter from J. Hilt to Students/Families, dated June 17, 2009 App. Tab 24. Although data is not available to show when tracking was deactivated for those laptops, Mr. Hilt advised us that all but three of the laptops were returned, and TheftTrack was deactivated, promptly.

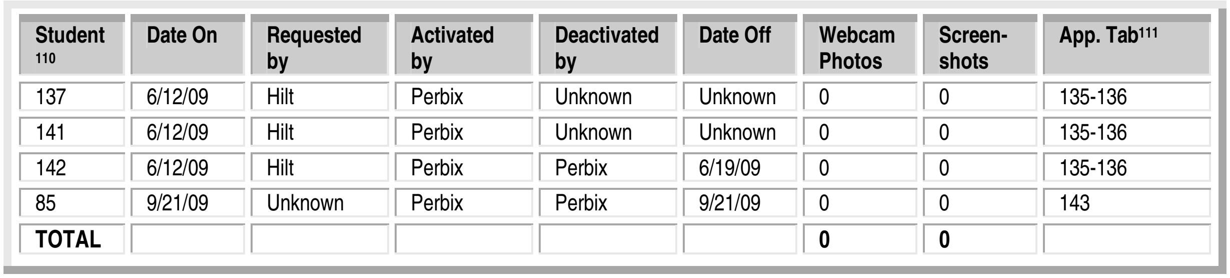
[109] Between September 29, 2008 and September 21, 2009, IP-only tracking was activated for laptops issued to eight students who were not allowed to take their laptops off-campus for disciplinary reasons. The duration of the IP-only tracking of those laptops was commensurate with the term of discipline.

[110] To protect the privacy of the individuals to whom laptops that were tracked were issued, we identify students herein using anonymous numbers. Laptops issued to teachers are similarly identified with "T[#]," classroom-based laptops are identified with "C[#]," and unassigned laptops are identified with "U[#]."

[111] Supporting documentation for each activation is reproduced at the Appendix Tab(s) noted in the far right column of the charts in this section of the Report.

Student[110]	Date On	Requested by	Activated by	Deactivated by	Date Off	Webcam Photos	Screen-shots	App. Tab[111]
13	9/29/08	Hilt	Perbix	Perbix	3/12/09	0	0	79-80
72	9/29/08	Hilt	Perbix	Perbix	3/12/09	0	0	79-80
82	9/29/08	Hilt	Perbix	Perbix	11/7/08	0	0	79-80
117	9/29/08	Hilt	Perbix	Perbix	11/7/08	0	0	79-80
124	9/29/08	Hilt	Perbix	Perbix	11/7/08	0	0	79-80
130	9/29/08	Hilt	Perbix	Perbix	3/12/09	0	0	79-80
3	10/2/08	Hilt	Perbix	Perbix	3/12/09	0	0	86, 111
5	10/2/08	Hilt	Perbix	Perbix	3/12/09	0	0	88
9	10/2/08	Hilt	Perbix	Perbix	3/12/09	0	0	88, 111
10	10/2/08	Hilt	Unknown	Perbix	3/12/09	0	0	86, 111
14	10/2/08	Hilt	Perbix	Perbix	3/12/09	0	0	83, 111
15	10/2/08	Hilt	Perbix	Perbix	3/12/09	0	0	84, 87
20	10/2/08	Hilt	Perbix	Perbix	3/12/09	0	0	88, 111
21	10/2/08	Hilt	Perbix	Perbix	3/12/09	0	0	111
23	10/2/08	Hilt	Perbix	Perbix	3/12/09	0	0	88, 111
24	10/2/08	Hilt	Perbix	Perbix	3/12/09	0	0	88, 111
34	10/2/08	Hilt	Perbix	Perbix	3/12/09	0	0	111
40	10/2/08	Hilt	Perbix	Perbix	3/12/09	0	0	86, 111
44	10/2/08	Hilt	Perbix	Perbix	3/1209	0	0	111
51	10/2/08	Hilt	Perbix	Perbix	3/12/09	0	0	111
62	10/2/08	Hilt	Perbix	Perbix	3/12/09	0	0	111
63	10/2/08	Hilt	Perbix	Perbix	3/12/09	0	0	88, 111
67	10/2/08	Hilt	Perbix	Perbix	3/12/09	0	0	83, 111
69	10/2/08	Hilt	Perbix	Perbix	3/12/09	0	0	88, 111
74	10/2/08	Hilt	Perbix	Perbix	3/12/09	0	0	88, 111
76	10/2/08	Hilt	Perbix	Perbix	3/12/09	0	0	88, 111
78	10/2/08	Hilt	Perbix	Perbix	3/12/09	0	0	88, 111
81	10/2/08	Hilt	Perbix	Perbix	3/12/09	0	0	88, 111
84	10/2/08	Hilt	Perbix	Perbix	3/12/09	0	0	86, 111
87	10/2/08	Hilt	Perbix	Perbix	3/12/09	0	0	86, 111
88	10/2/08	Hilt	Perbix	Perbix	3/12/09	0	0	88
89	10/2/08	Hilt	Perbix	Perbix	10/6/08	0	0	88, 111
92	10/2/08	Hilt	Perbix	Perbix	3/12/09	0	0	88, 111
101	10/2/08	Hilt	Perbix	Perbix	3/12/09	0	0	88, 111
105	10/2/08	Hilt	Perbix	Perbix	3/12/09	0	0	81, 111
107	10/2/08	Hilt	Perbix	Perbix	3/12/09	0	0	111
114	10/2/08	Hilt	Perbix	Perbix	3/12/09	0	0	81, 111
126	10/2/08	Hilt	Perbix	Perbix	3/12/09	0	0	86, 111
127	10/2/08	Hilt	Perbix	Perbix	3/12/09	0	0	86, 111
131	10/2/08	Hilt	Perbix	Perbix	3/12/09	0	0	88, 111
138	10/2/08	Hilt	Perbix	Perbix	3/12/09	0	0	88, 111
70	10/3/08	Hilt	Perbix	Perbix	3/12/09	0	0	90, 111
75	10/3/08	Hilt	Perbix	Perbix	3/12/09	0	0	90, 111
80	10/3/08	Hilt	Perbix	Perbix	3/12/09	0	0	90
103	10/3/08	Hilt	Perbix	Perbix	3/12/09	0	0	89, 111
132	10/3/08	Hilt	Perbix	Perbix	3/12/09	0	0	90, 111

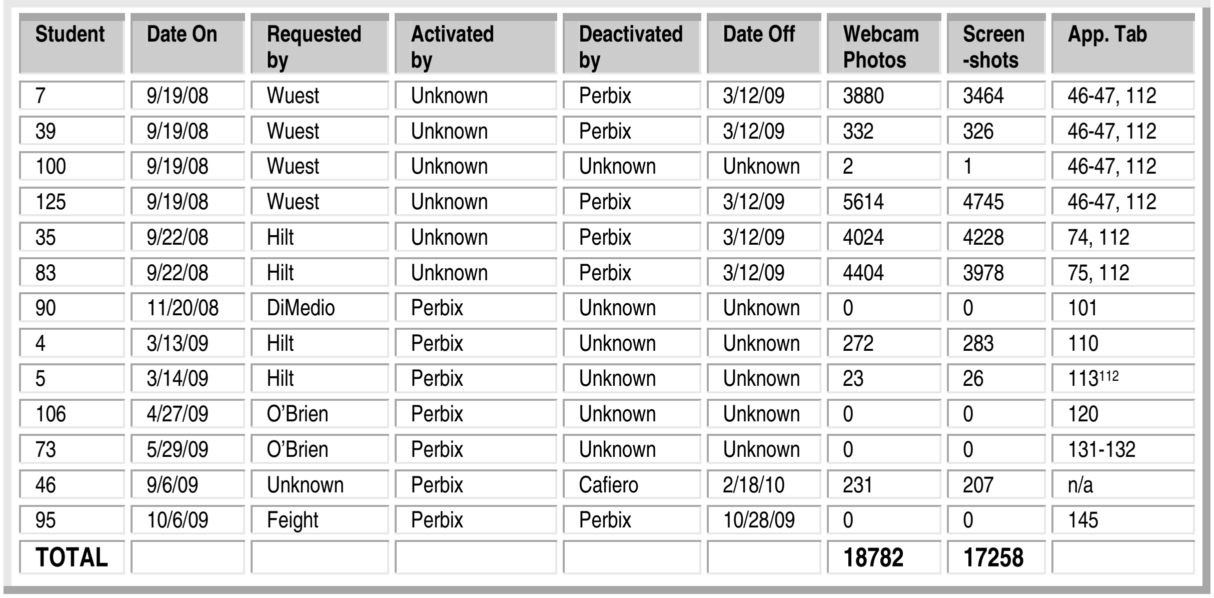
Student[110]	Date On	Requested by	Activated by	Deactivated by	Date Off	Webcam Photos	Screen-shots	App. Tab[111]
77	10/4/08	Hilt	Perbix	Perbix	3/12/09	0	0	92
115	10/4/08	Hilt	Perbix	Perbix	3/12/09	0	0	92
122	10/4/08	Hilt	Perbix	Perbix	3/12/09	0	0	92, 111
49	10/5/08	Hilt	Perbix	Perbix	3/12/09	0	0	93, 111
66	10/6/08	Hilt	Perbix	Perbix	3/12/09	0	0	111
76	5/19/09	Hilt	Perbix	Perbix	5/20/09	0	0	127
3	6/3/09	Hilt	Perbix	Unknown	Unknown	0	0	133
20	6/3/09	Hilt	Perbix	Unknown	Unknown	0	0	133
23	6/3/09	Hilt	Perbix	Unknown	Unknown	0	0	133
27	6/3/09	Hilt	Perbix	Unknown	Unknown	0	0	133
32	6/3/09	Hilt	Perbix	Unknown	Unknown	0	0	133
40	6/3/09	Hilt	Perbix	Unknown	Unknown	0	0	133
44	6/3/09	Hilt	Perbix	Unknown	Unknown	0	0	133
66	6/3/09	Hilt	Perbix	Unknown	6/10/09	0	0	133
74	6/3/09	Hilt	Perbix	Unknown	Unknown	0	0	133
78	6/3/09	Hilt	Perbix	Unknown	Unknown	0	0	133
79	6/3/09	Hilt	Perbix	Unknown	Unknown	0	0	133
81	6/3/09	Hilt	Perbix	Unknown	Unknown	0	0	133
98	6/3/09	Hilt	Perbix	Unknown	Unknown	0	0	133
101	6/3/09	Hilt	Perbix	Unknown	Unknown	0	0	133
122	6/3/09	Hilt	Perbix	Unknown	Unknown	0	0	133
126	6/3/09	Hilt	Perbix	Unknown	Unknown	0	0	133
127	6/3/09	Hilt	Perbix	Unknown	Unknown	0	0	133
126	6/11/09	O'Brien	Perbix	Unknown	Unknown	0	0	n/a
11	6/12/09	Hilt	Perbix	Unknown	Unknown	0	0	135-136
28	6/12/09	Hilt	Perbix	Unknown	Unknown	0	0	135-136
37	6/12/09	Hilt	Perbix	Unknown	Unknown	0	0	135-136
38	6/12/09	Hilt	Perbix	Unknown	Unknown	0	0	135-136
54	6/12/09	Hilt	Perbix	Unknown	Unknown	0	0	135-136
55	6/12/09	Hilt	Perbix	Unknown	Unknown	0	0	135-136
60	6/12/09	Hilt	Perbix	Unknown	Unknown	0	0	135-136
61	6/12/09	Hilt	Perbix	Unknown	Unknown	0	0	135-136
64	6/12/09	Hilt	Perbix	Unknown	Unknown	0	0	135-136
86	6/12/09	Hilt	Perbix	Unknown	Unknown	0	0	135-136
91	6/12/09	Hilt	Perbix	Unknown	Unknown	0	0	135-136
93	6/12/09	Hilt	Perbix	Perbix	6/19/09	0	0	135-136
102	6/12/09	Hilt	Perbix	Unknown	Unknown	0	0	135-136
106	6/12/09	Hilt	Perbix	Unknown	Unknown	0	0	135-136
107	6/12/09	Hilt	Perbix	Perbix	6/19/09	0	0	135-136
108	6/12/09	Hilt	Perbix	Unknown	Unknown	0	0	135-136
109	6/12/09	Hilt	Perbix	Unknown	Unknown	0	0	135-136
118	6/12/09	Hilt	Perbix	Perbix	Unknown	0	0	135-136
119	6/12/09	Hilt	Perbix	Unknown	Unknown	0	0	135-136
120	6/12/09	Hilt	Perbix	Perbix	9/9/09	0	0	135-136
126	6/12/09	Hilt	Perbix	Unknown	Unknown	0	0	135-136
128	6/12/09	Hilt	Perbix	Unknown	Unknown	0	0	135-136



Student[110]	Date On	Requested by	Activated by	Deactivated by	Date Off	Webcam Photos	Screen-shots	App. Tab[111]
137	6/12/09	Hilt	Perbix	Unknown	Unknown	0	0	135-136
141	6/12/09	Hilt	Perbix	Unknown	Unknown	0	0	135-136
142	6/12/09	Hilt	Perbix	Perbix	6/19/09	0	0	135-136
85	9/21/09	Unknown	Perbix	Perbix	9/21/09	0	0	143
TOTAL						**0**	**0**	

2. Stolen Student Laptops

Between September 19, 2008 and February 18, 2010, TheftTrack was activated on 13 student laptops that were reported stolen. Six of those laptops were recovered by the Lower Merion Police Department. Those trackings resulted in the capture of 18,782 webcam photographs and 17,258 screenshots that were recovered in the investigation.



Student	Date On	Requested by	Activated by	Deactivated by	Date Off	Webcam Photos	Screen -shots	App. Tab
7	9/19/08	Wuest	Unknown	Perbix	3/12/09	3880	3464	46-47, 112
39	9/19/08	Wuest	Unknown	Perbix	3/12/09	332	326	46-47, 112
100	9/19/08	Wuest	Unknown	Unknown	Unknown	2	1	46-47, 112
125	9/19/08	Wuest	Unknown	Perbix	3/12/09	5614	4745	46-47, 112
35	9/22/08	Hilt	Unknown	Perbix	3/12/09	4024	4228	74, 112
83	9/22/08	Hilt	Unknown	Perbix	3/12/09	4404	3978	75, 112
90	11/20/08	DiMedio	Perbix	Unknown	Unknown	0	0	101
4	3/13/09	Hilt	Perbix	Unknown	Unknown	272	283	110
5	3/14/09	Hilt	Perbix	Unknown	Unknown	23	26	113[112]
106	4/27/09	O'Brien	Perbix	Unknown	Unknown	0	0	120
73	5/29/09	O'Brien	Perbix	Unknown	Unknown	0	0	131-132
46	9/6/09	Unknown	Perbix	Cafiero	2/18/10	231	207	n/a
95	10/6/09	Feight	Perbix	Perbix	10/28/09	0	0	145
TOTAL						**18782**	**17258**	

Most of the recovered images for the laptops in this category (34,998 of the 36,040 images) were captured by the 6 laptops that were stolen from an HHS locker room on September 19, 2008. TheftTrack was activated for four of those laptops the same day (the initial

[112] As reflected in the supporting e-mail, this activation arose from an apparent suspicion about the accuracy of the report of theft that gave rise to a TheftTrack activation on the prior day. *See* E-mail from J. Hilt to M. Perbix, March 13, 2009, App. Tab 113.

report received by the IS Department was that four laptops had been stolen, not six).[113] Within the next hour, Ms. Cafiero sent images captured by LANrev from two of the stolen laptops to a group of IS personnel and Mr. Witt.[114] The images were made available to the Lower Merion Police Department via a secure, password-protected portion of LMSD's website.[115] The police recovered two of the laptops on September 24, 2008 and the remaining four on September 26, 2008. They returned all six laptops to LMSD on October 9, 2008.

In what appears to us to have been a major oversight, TheftTrack remained activated on the six laptops after they were returned. Our review of the images captured by the laptops suggests that the laptops were in the possession of the IS Department from October 13, 2008 to November 11, 2008, and reissued to students between October 15 and November 17, 2008. Tracking for five of the six laptops, however, continued until March 12, 2009, when Mr. Perbix purged the LANrev database for maintenance reasons. On September 29, 2008, Mr. Perbix had asked Mr. O'Brien whether tracking should continue for several listed laptops, which included those that had been stolen from the locker room, and Mr. O'Brien responded that it should, even though there is evidence that he knew then that the stolen laptops were in the possession of the police at that time.[116] Our investigation has revealed no explanation why Mr. O'Brien responded as he did, and there is no evidence that Mr. Perbix checked with Mr. O'Brien

[113] *See* E-Mails between C. Cafiero and IS personnel, dated September 19, 2008, App. Tab 46.

[114] *See* E-Mail from C. Cafiero to IS personnel and D. Witt, dated September 19, 2008, App. Tab 47.

[115] *See* E-mails from D. Witt to Det. Craig, dated September 19, 2008, App. Tabs 48-49; E-mail from J. Valentine to Det. Craig, et al., dated September 23, 2008, App. Tab 49.

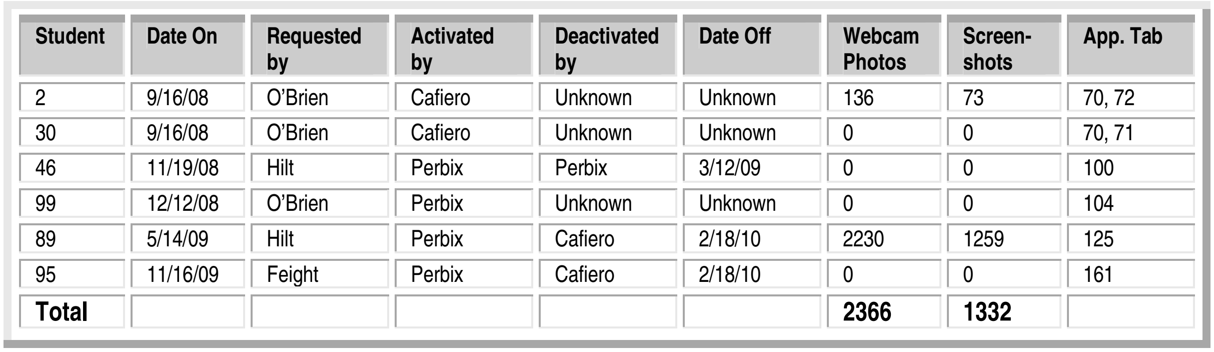
[116] *See* E-mails between M. Perbix and K. O'Brien, dated September 29, 2008, App. Tab 80; E-mail from C. Cafiero to K. O'Brien, et al., dated September 26, 2008, App. Tab 77.

again about whether TheftTrack should remain activated. While back in the possession of students and until March 12, 2009, TheftTrack continued to capture webcam photographs and screenshots: 18,241 webcam photographs and 16,732 screenshots. Data showing when tracking was deactivated for the sixth laptop is unavailable, as are any images that were captured from that laptop after it was returned to LMSD.

No images from four of the six other stolen laptops were recovered in the investigation, possibly because after they were stolen the laptops were not connected to the Internet or their hard drives were reformatted.[117]

3. Laptops Not Returned By Students Who Withdrew from School

Between September 16, 2008 and February 18, 2010, TheftTrack was activated on six student laptops after the students withdrew from school without returning their laptops. Those trackings resulted in 2,366 webcam photographs and 1,332 screenshots that were recovered in the investigation, and the laptops were not recovered. In any event, the wisdom and propriety of activating image tracking in these circumstances are questionable at best.

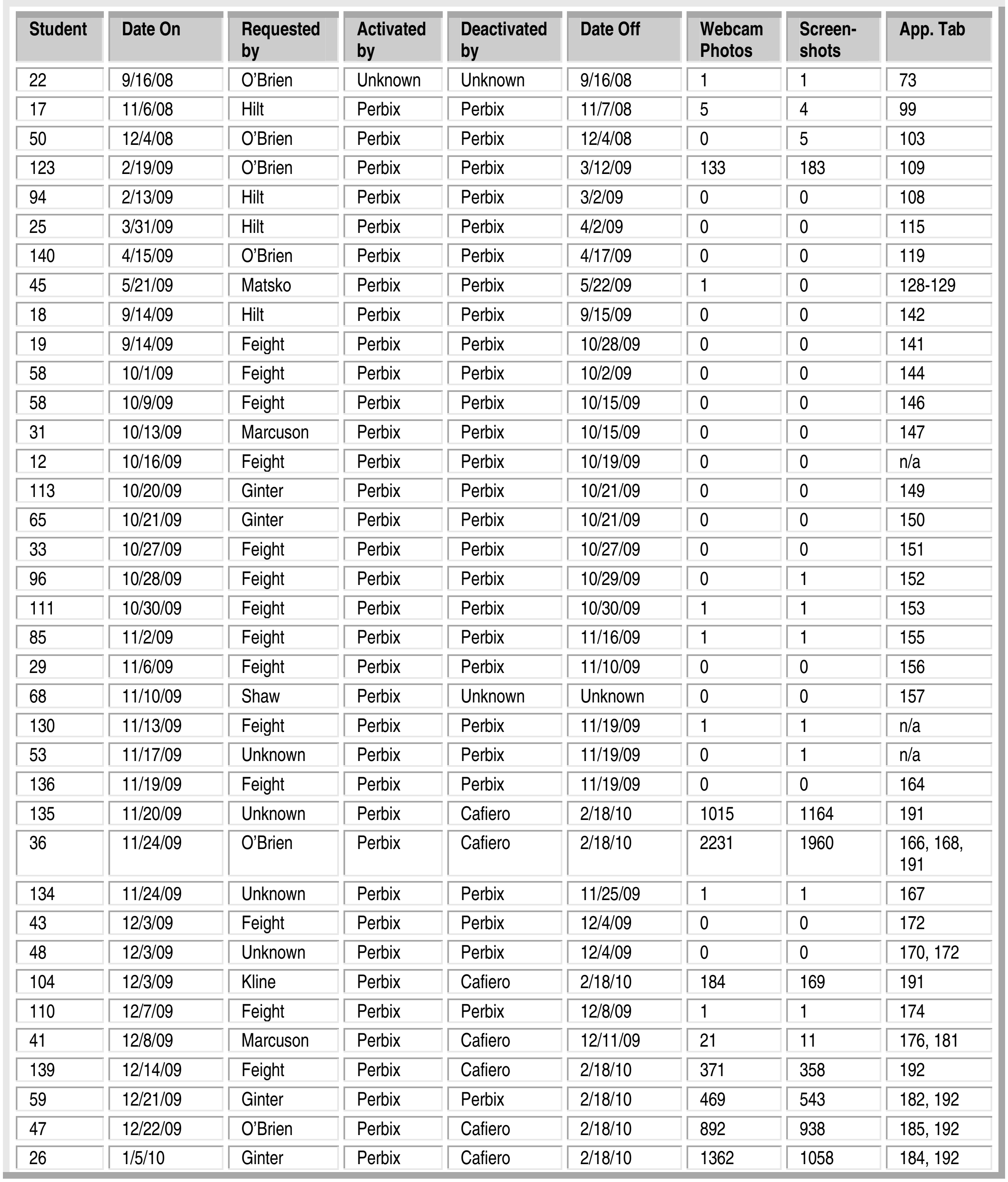


Student	Date On	Requested by	Activated by	Deactivated by	Date Off	Webcam Photos	Screen-shots	App. Tab
2	9/16/08	O'Brien	Cafiero	Unknown	Unknown	136	73	70, 72
30	9/16/08	O'Brien	Cafiero	Unknown	Unknown	0	0	70, 71
46	11/19/08	Hilt	Perbix	Perbix	3/12/09	0	0	100
99	12/12/08	O'Brien	Perbix	Unknown	Unknown	0	0	104
89	5/14/09	Hilt	Perbix	Cafiero	2/18/10	2230	1259	125
95	11/16/09	Feight	Perbix	Cafiero	2/18/10	0	0	161
Total						**2366**	**1332**	

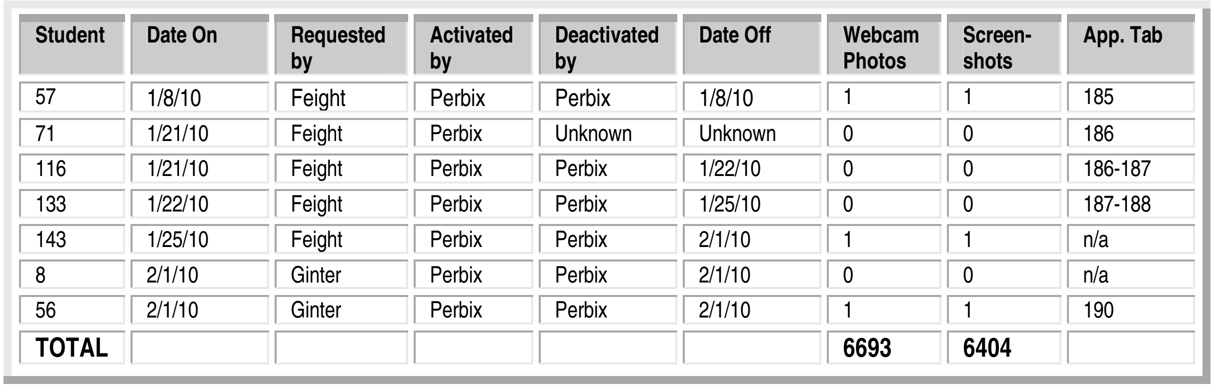
[117] *See* LANrev User Guide Mac OS X Admin. Version 6, at 114, App. Tab 202.

4. Missing Student Laptops

Between September 16, 2008 and February 18, 2010, TheftTrack was activated on 44 laptops that were reported missing, resulting in the capture of 6,693 webcam photographs and 6,404 screenshots that were recovered in the investigation.



Student	Date On	Requested by	Activated by	Deactivated by	Date Off	Webcam Photos	Screen-shots	App. Tab
22	9/16/08	O'Brien	Unknown	Unknown	9/16/08	1	1	73
17	11/6/08	Hilt	Perbix	Perbix	11/7/08	5	4	99
50	12/4/08	O'Brien	Perbix	Perbix	12/4/08	0	5	103
123	2/19/09	O'Brien	Perbix	Perbix	3/12/09	133	183	109
94	2/13/09	Hilt	Perbix	Perbix	3/2/09	0	0	108
25	3/31/09	Hilt	Perbix	Perbix	4/2/09	0	0	115
140	4/15/09	O'Brien	Perbix	Perbix	4/17/09	0	0	119
45	5/21/09	Matsko	Perbix	Perbix	5/22/09	1	0	128-129
18	9/14/09	Hilt	Perbix	Perbix	9/15/09	0	0	142
19	9/14/09	Feight	Perbix	Perbix	10/28/09	0	0	141
58	10/1/09	Feight	Perbix	Perbix	10/2/09	0	0	144
58	10/9/09	Feight	Perbix	Perbix	10/15/09	0	0	146
31	10/13/09	Marcuson	Perbix	Perbix	10/15/09	0	0	147
12	10/16/09	Feight	Perbix	Perbix	10/19/09	0	0	n/a
113	10/20/09	Ginter	Perbix	Perbix	10/21/09	0	0	149
65	10/21/09	Ginter	Perbix	Perbix	10/21/09	0	0	150
33	10/27/09	Feight	Perbix	Perbix	10/27/09	0	0	151
96	10/28/09	Feight	Perbix	Perbix	10/29/09	0	1	152
111	10/30/09	Feight	Perbix	Perbix	10/30/09	1	1	153
85	11/2/09	Feight	Perbix	Perbix	11/16/09	1	1	155
29	11/6/09	Feight	Perbix	Perbix	11/10/09	0	0	156
68	11/10/09	Shaw	Perbix	Unknown	Unknown	0	0	157
130	11/13/09	Feight	Perbix	Perbix	11/19/09	1	1	n/a
53	11/17/09	Unknown	Perbix	Perbix	11/19/09	0	1	n/a
136	11/19/09	Feight	Perbix	Perbix	11/19/09	0	0	164
135	11/20/09	Unknown	Perbix	Cafiero	2/18/10	1015	1164	191
36	11/24/09	O'Brien	Perbix	Cafiero	2/18/10	2231	1960	166, 168, 191
134	11/24/09	Unknown	Perbix	Perbix	11/25/09	1	1	167
43	12/3/09	Feight	Perbix	Perbix	12/4/09	0	0	172
48	12/3/09	Unknown	Perbix	Perbix	12/4/09	0	0	170, 172
104	12/3/09	Kline	Perbix	Cafiero	2/18/10	184	169	191
110	12/7/09	Feight	Perbix	Perbix	12/8/09	1	1	174
41	12/8/09	Marcuson	Perbix	Cafiero	12/11/09	21	11	176, 181
139	12/14/09	Feight	Perbix	Cafiero	2/18/10	371	358	192
59	12/21/09	Ginter	Perbix	Perbix	2/18/10	469	543	182, 192
47	12/22/09	O'Brien	Perbix	Cafiero	2/18/10	892	938	185, 192
26	1/5/10	Ginter	Perbix	Cafiero	2/18/10	1362	1058	184, 192



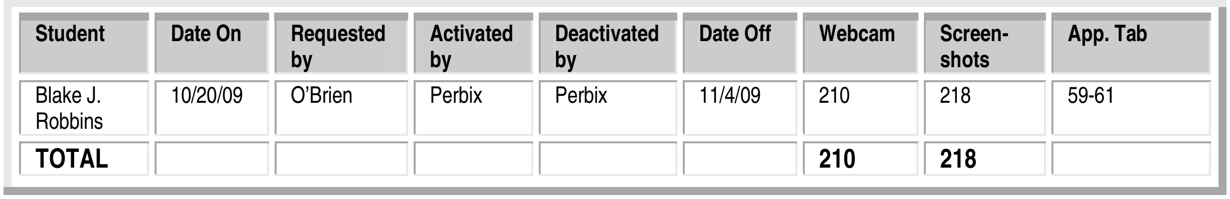
Student	Date On	Requested by	Activated by	Deactivated by	Date Off	Webcam Photos	Screen-shots	App. Tab
57	1/8/10	Feight	Perbix	Perbix	1/8/10	1	1	185
71	1/21/10	Feight	Perbix	Unknown	Unknown	0	0	186
116	1/21/10	Feight	Perbix	Perbix	1/22/10	0	0	186-187
133	1/22/10	Feight	Perbix	Perbix	1/25/10	0	0	187-188
143	1/25/10	Feight	Perbix	Perbix	2/1/10	1	1	n/a
8	2/1/10	Ginter	Perbix	Perbix	2/1/10	0	0	n/a
56	2/1/10	Ginter	Perbix	Perbix	2/1/10	1	1	190
TOTAL						**6693**	**6404**	

Thus, 12,361 of the 13,097 recovered images from the laptops in this category were captured from 6 laptops. TheftTrack remained activated on those laptops for between 17 days and 6 weeks after the laptops were found. We have not found any definitive explanation for why those trackings continued, but the likely explanations reflect the lack of formal policies and procedures: (i) the student did not report to the building-level technician at his or her school that he or she had found the laptop; (ii) the building-level technician failed to advise Ms. Cafiero or Mr. Perbix that TheftTrack should be deactivated; or (iii) Ms. Cafiero and/or Mr. Perbix failed to deactivate TheftTrack after learning that the laptop had been found. We note that we found no evidence of any surreptitious or nefarious downloading of any images from the LANrev inventory server.

5. Image-Tracking of Laptop for Which Insurance Fees Were Unpaid

On October 20, 2009, Blake J. Robbins brought his One-to-One laptop to the HHS Help Desk with a broken screen and was issued a loaner laptop. Later that morning, Building-Level Technician Kyle O’Brien, Desktop Technician Chuck Ginter, and Rhonda Keefer, the teacher liaison to the One-to-One program, conferred and agreed that Mr. Robbins should not have been issued a loaner laptop in light of outstanding insurance fees. Mr. Ginter then e-mailed Ms. Matsko and informed her that "we need to retrieve the laptop ASAP."[118]

There is a conflict between HHS Assistant Principal Lindy Matsko and Mr. O'Brien about who directed Mr. O'Brien to have tracking activated: Mr. O'Brien testified at his deposition in the Robbins lawsuit that Ms. Matsko instructed him to have TheftTrack activated; Ms. Matsko testified at her deposition that she did not authorize tracking. In any event, at 1:10 p.m. on October 20, 2009, Mr. O'Brien e-mailed Mr. Perbix and directed him to activate TheftTrack on Mr. Robbins's loaner laptop.[119] At 3:55 p.m., Mr. Perbix advised Mr. O'Brien by e-mail that the laptop was "[n]ow currently online at home."[120] The next day, Mr. Perbix asked Mr. O'Brien whether he should continue tracking the laptop.[121] Mr. O'Brien responded "yes."[122] Mr. O'Brien told us that he believed that he needed authorization from Ms. Matsko, which he never requested or received, to terminate tracking. Consequently, the loaner laptop was tracked from October 20, 2009 to November 4, 2009, resulting in the capture of 210 webcam photographs and 218 screenshots that were recovered in the investigation.



Student	Date On	Requested by	Activated by	Deactivated by	Date Off	Webcam	Screen-shots	App. Tab
Blake J. Robbins	10/20/09	O'Brien	Perbix	Perbix	11/4/09	210	218	59-61
TOTAL						**210**	**218**	

[118] E-mails between G. Ginter and L. Matsko et al., dated October 20, 2009, App. Tab 59.

[119] E-mail from K. O'Brien to M. Perbix, dated October 20, 2009, App. Tab 60.

[120] E-mails between M. Perbix and K. O'Brien, dated October 20, 2009, App. Tab 61.

[121] E-mails between M. Perbix and K. O'Brien, dated October 21, 2009, App. Tab 62.

[122] E-mail between M. Perbix to K. O'Brien, dated October 21, 2009, App. Tab 62.

On or about October 26, 2009, Mr. Perbix observed a screenshot from the loaner laptop. The screenshot included an on-line chat that concerned him. On or about October 30, 2009, Mr. Perbix showed that image to Mr. Frazier. After consulting with Mr. Frazier, on October 30, 2009, Mr. Perbix set up a folder in the LMSD network home directories of HHS Principal Steve Kline and Ms. Matsko to enable them to view the images captured from the laptop issued to Mr. Robbins.[123]

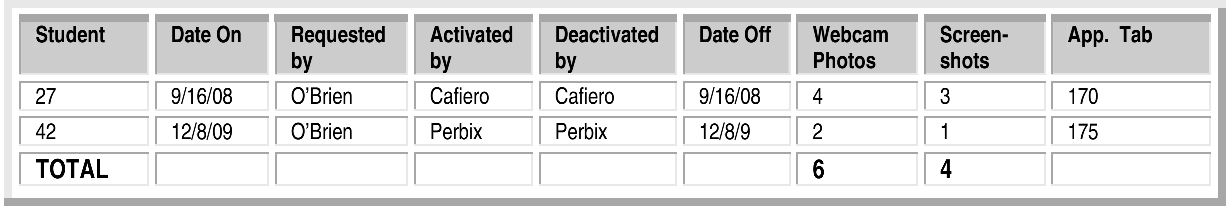
On November 2 or 3, 2009, Ms. Matsko and Mr. Kline, in a meeting also attended by HHS Assistant Principal Lauren Marcuson, discussed certain images captured from Blake Robbins's loaner laptop. According to Ms. Matsko, Mr. Kline advised her that unless there was additional evidence that gave them a contextual basis for doing so, school officials should not discuss the images with the student or his parents because they involved off-campus activities. Ms. Matsko ultimately decided, about one week later, that it was appropriate to discuss certain seemingly troubling images with Mr. Robbins and/or his parents. The substance of the conversation or conversations in which she did so is disputed. In that regard, it bears noting that the Robbinses have not been interviewed or deposed.

Mr. Robbins was not disciplined as a result of any images captured from his laptop.

6. Mistaken Activations for Student Laptops

TheftTrack was activated on the wrong laptop twice: once on September 16, 2008 and once on December 8, 2009. Those trackings resulted in the capture of six webcam photographs and four screenshots that were recovered in the investigation.

[123] E-mails between S. Kline and M. Perbix, et al., dated October 30, 2009, App. Tab 63.



Student	Date On	Requested by	Activated by	Deactivated by	Date Off	Webcam Photos	Screen-shots	App. Tab
27	9/16/08	O'Brien	Cafiero	Cafiero	9/16/08	4	3	170
42	12/8/09	O'Brien	Perbix	Perbix	12/8/9	2	1	175
TOTAL						**6**	**4**	

The first mistaken activation resulted from misinformation provided to Mr. O'Brien about a student who supposedly had withdrawn from school without returning the laptop. On September 16, 2008, Mr. O'Brien e-mailed Mr. Perbix, Ms. Cafiero and Ms. DiMedio to report that a particular student had withdrawn and had not returned her laptop, and wrote: "Mike if you want to start tracking the laptop let me know and I will give you computer names and serial numbers." Fifteen minutes after Ms. Cafiero activated TheftTrack, Mr. O'Brien e-mailed the group, explaining that he had received misinformation and that the student in fact had not withdrawn. About four hours later, Ms. Cafiero advised Mr. O'Brien that she would deactivate TheftTrack.[124]

The second mistaken activation resulted from Mr. O'Brien's misspelling of the name of the student for whom he asked Mr. Perbix to activate TheftTrack (two students had similar names). Mr. O'Brien caught the mistake after about 20 minutes and directed Mr. Perbix to deactivate TheftTrack.[125]

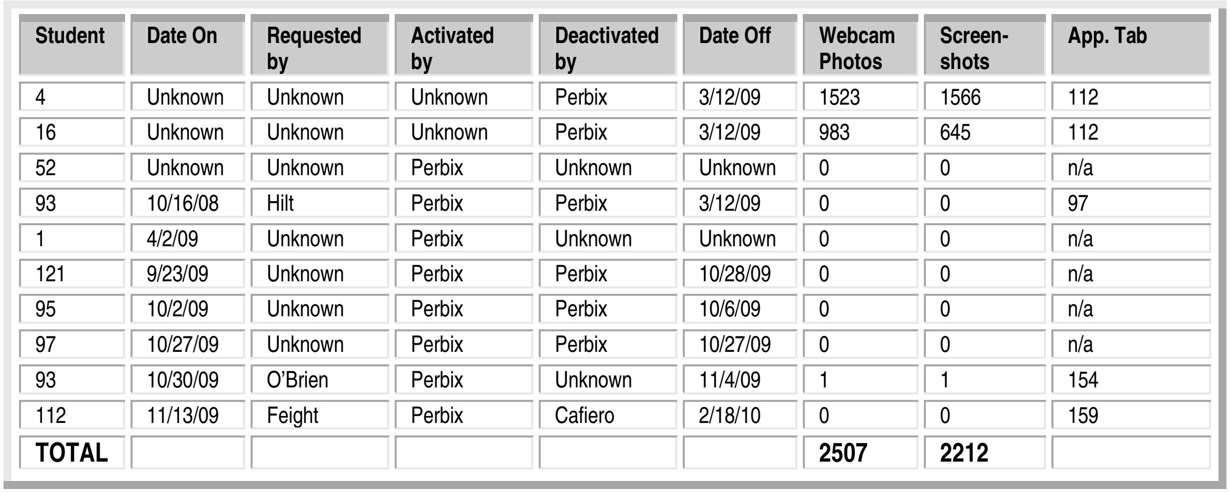
7. Activations for Student Laptops for Reasons Unknown

There are 10 activations of TheftTrack on student laptops for which there is insufficient evidence to establish why tracking was activated. The tracking of those laptops

[124] *See* E-mails between K. O'Brien and C. Cafiero, et al., dated September 16, 2008, App. Tab 71.

[125] *See* E-mails between K. O'Brien and M. Perbix, dated December 8, 2009, App. Tab 176.

resulted in the capture of 2,507 webcam photographs and 2,212 screenshots that were recovered in the investigation.



Student	Date On	Requested by	Activated by	Deactivated by	Date Off	Webcam Photos	Screen-shots	App. Tab
4	Unknown	Unknown	Unknown	Perbix	3/12/09	1523	1566	112
16	Unknown	Unknown	Unknown	Perbix	3/12/09	983	645	112
52	Unknown	Unknown	Perbix	Unknown	Unknown	0	0	n/a
93	10/16/08	Hilt	Perbix	Perbix	3/12/09	0	0	97
1	4/2/09	Unknown	Perbix	Unknown	Unknown	0	0	n/a
121	9/23/09	Unknown	Perbix	Perbix	10/28/09	0	0	n/a
95	10/2/09	Unknown	Perbix	Perbix	10/6/09	0	0	n/a
97	10/27/09	Unknown	Perbix	Perbix	10/27/09	0	0	n/a
93	10/30/09	O'Brien	Perbix	Unknown	11/4/09	1	1	154
112	11/13/09	Feight	Perbix	Cafiero	2/18/10	0	0	159
TOTAL						**2507**	**2212**	

For 3 of these 10 activations, we found e-mails from Mr. Hilt, Mr. O'Brien, or Mr. Feight to Mr. Perbix requesting that he activate TheftTrack without stating a reason for doing so.[126] This is a reflection of the deficiencies in the District's policies and procedures. The tracking of those 3 laptops resulted in the capture of 1 webcam photograph and 1 screenshot that were recovered in the investigation.

Also, of the 10 unexplained activations, only 3 resulted in images that were recovered. Although there is no forensic evidence to establish when tracking began for the laptop that returned the most recovered images, our review of the images suggests that the laptop was tracked while in the possession of the student to whom it was assigned from November 17, 2008 until tracking was deactivated on March 12, 2008. This, again, appears to be a major oversight.

[126] *See* App. Tabs 97, 154, and 159.

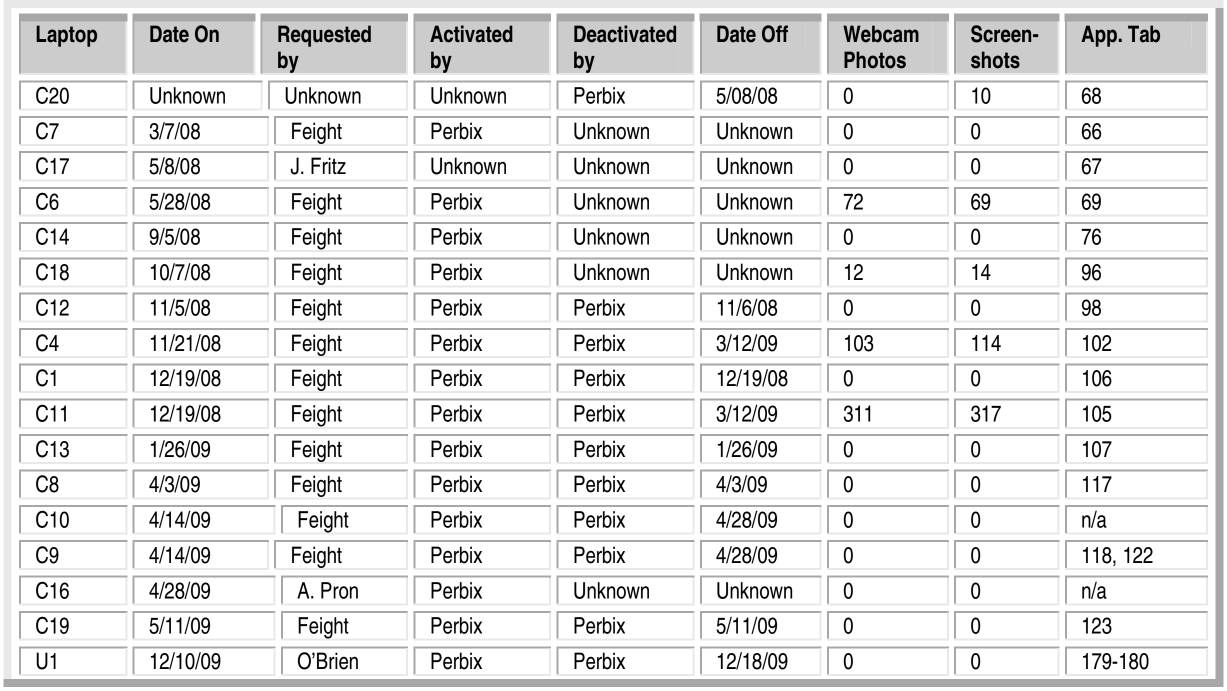
8. Classroom and Unassigned Loaner Laptops

Between March 7, 2008 and February 18, 2010, TheftTrack was activated on 25 classroom or unassigned loaner laptops, resulting in the capture of 527 webcam photographs and 551 screenshots that were recovered in the investigation.

a. Laptops Reported Stolen or Missing

Of the 25 activations for classroom or unassigned loaner laptops, 17 arose from a report that the laptop was stolen or missing. The tracking of the 17 laptops resulted in the capture of 498 webcam photographs and 524 screenshots that were recovered in the investigation. All of the images were captured from four classroom laptops that had been reported missing. Three laptops captured webcam photographs of students and teachers in classrooms and contemporaneous screenshots and one laptop captured blank webcam photographs.

Three of the seventeen laptops were reported stolen. The investigation revealed neither any images from those laptops nor any evidence that the laptops were recovered.



Laptop	Date On	Requested by	Activated by	Deactivated by	Date Off	Webcam Photos	Screen-shots	App. Tab
C20	Unknown	Unknown	Unknown	Perbix	5/08/08	0	10	68
C7	3/7/08	Feight	Perbix	Unknown	Unknown	0	0	66
C17	5/8/08	J. Fritz	Unknown	Unknown	Unknown	0	0	67
C6	5/28/08	Feight	Perbix	Unknown	Unknown	72	69	69
C14	9/5/08	Feight	Perbix	Unknown	Unknown	0	0	76
C18	10/7/08	Feight	Perbix	Unknown	Unknown	12	14	96
C12	11/5/08	Feight	Perbix	Perbix	11/6/08	0	0	98
C4	11/21/08	Feight	Perbix	Perbix	3/12/09	103	114	102
C1	12/19/08	Feight	Perbix	Perbix	12/19/08	0	0	106
C11	12/19/08	Feight	Perbix	Perbix	3/12/09	311	317	105
C13	1/26/09	Feight	Perbix	Perbix	1/26/09	0	0	107
C8	4/3/09	Feight	Perbix	Perbix	4/3/09	0	0	117
C10	4/14/09	Feight	Perbix	Perbix	4/28/09	0	0	n/a
C9	4/14/09	Feight	Perbix	Perbix	4/28/09	0	0	118, 122
C16	4/28/09	A. Pron	Perbix	Unknown	Unknown	0	0	n/a
C19	5/11/09	Feight	Perbix	Perbix	5/11/09	0	0	123
U1	12/10/09	O'Brien	Perbix	Perbix	12/18/09	0	0	179-180

TOTAL						**498**	**524**	

b. Activations for Reasons Unknown

There is no evidence to determine the reasons for eight activations for classroom and unassigned loaner laptops. Those activations resulted in the capture of 28 webcam photographs and 26 screenshots that were recovered in the investigation. Those images were captured from four classroom laptops. The webcam photographs show students and teachers in a classroom.

Laptop No.	Date On	Requested by	Activated by	Deactivated by	Date Off	Webcam	Screen-shots	App. Tab
C21	Unknown	Unknown	Unknown	Unknown	Unknown	0	0	n/a
C22	Unknown	Unknown	Unknown	Unknown	Unknown	1	1	n/a
U2	Unknown	Unknown	Unknown	Perbix	3/12/09	0	0	n/a
C5	3/7/08	Unknown	Unknown	Unknown	Unknown	26	24	66
U4	12/12/08	Unknown	Perbix	Perbix	5/11/09	0	0	n/a
C2	4/28/09	Feight	Perbix	Perbix	4/28/09	0	0	122-123
C3	4/28/09	Feight	Perbix	Perbix	4/28/09	0	0	122-123
C15	5/22/09	Feight	Perbix	Cafiero	2/18/10	1	1	130
TOTAL						**28**	**26**	

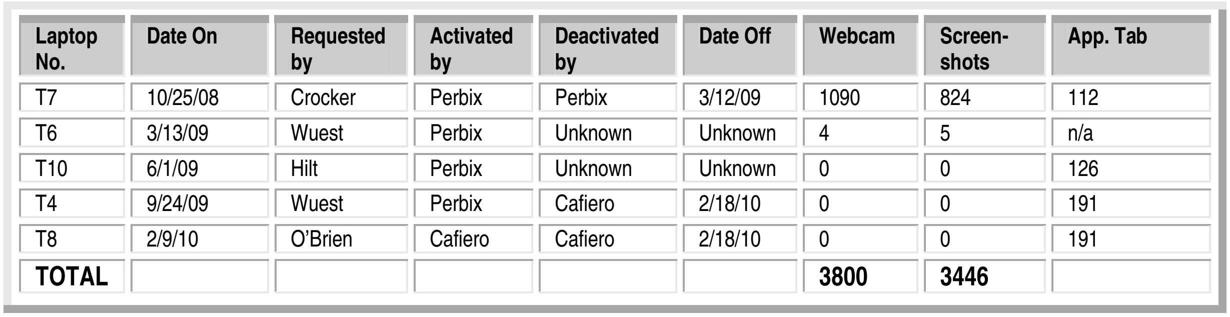
9. Teacher Laptops

Between December 1, 2007 and February 9, 2010, TheftTrack was activated on 12 laptops that were issued to teachers, resulting in the capture of 3,805 webcam photographs and 3,451 screenshots that were recovered in the investigation.

a. Laptops Reported Stolen

Six of the tracked teacher laptops were reported stolen. Tracking these stolen laptops resulted in the capture of 3,800 webcam photographs and 3,446 screenshots that were recovered in the investigation.

Laptop No.	Date On	Requested by	Activated by	Deactivated by	Date Off	Webcam	Screen-shots	App. Tab
T2	12/17/07	Unknown	Perbix	Unknown	Unknown	2706	2617	65



Laptop No.	Date On	Requested by	Activated by	Deactivated by	Date Off	Webcam	Screen-shots	App. Tab
T7	10/25/08	Crocker	Perbix	Perbix	3/12/09	1090	824	112
T6	3/13/09	Wuest	Perbix	Unknown	Unknown	4	5	n/a
T10	6/1/09	Hilt	Perbix	Unknown	Unknown	0	0	126
T4	9/24/09	Wuest	Perbix	Cafiero	2/18/10	0	0	191
T8	2/9/10	O'Brien	Cafiero	Cafiero	2/18/10	0	0	191
TOTAL						**3800**	**3446**	

More than 73% of the images were captured from a single laptop (T2) that was stolen from the car of a teacher at Belmont Hills Elementary School on December 7, 2007. Mr. Perbix and Ms. Cafiero worked with the Lower Merion Police Department to recover the laptop.[127] For the next year, the TheftTrack captured images and IP addresses, enabling the police to track the laptop from Lansdowne, Pennsylvania to Pakistan, and eventually back to Lansdowne, where it was recovered by the Lower Merion Police Department.[128] The Montgomery County District Attorney's Office prosecuted the person responsible for the theft.

Tracking of the other five stolen teacher laptops resulted in the capture of 1,094 webcam photographs and 829 screenshots that were recovered in the investigation. One of those laptops (T10) was reported found within two days; we have no evidence that the other four were found or recovered.

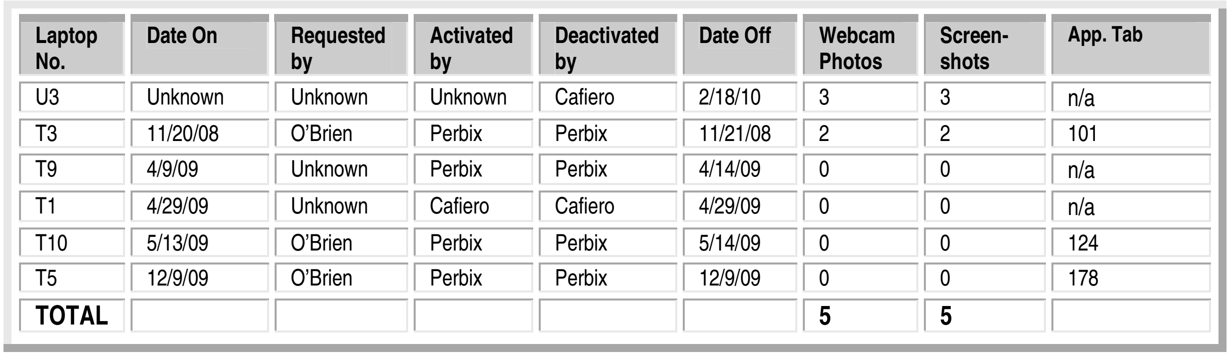
b. Activations for Reasons Unknown

There is no evidence to determine the reasons for six activations for teacher laptops. Those trackings resulted in the capture of five webcam photographs and five

[127] *See* E-mails between M. Perbix and V. DiMedio, dated December 17, 2007, App. Tab 65; E-mails between M. Perbix and C. Cafiero, et al., dated January 15, 2008, App. Tab 34.

[128] *See* E-mails between M. Perbix and C. Cafiero, dated September 18, 2008, App. Tab. 44; E-mail from M. Perbix to Technology Group, dated December 5, 2008, App. Tab 53.

screenshots that were recovered in the investigation. (The photographs from T3 appear to have been taken in a classroom; it is unclear where the photographs from U3 were taken.)



Laptop No.	Date On	Requested by	Activated by	Deactivated by	Date Off	Webcam Photos	Screen-shots	App. Tab
U3	Unknown	Unknown	Unknown	Cafiero	2/18/10	3	3	n/a
T3	11/20/08	O'Brien	Perbix	Perbix	11/21/08	2	2	101
T9	4/9/09	Unknown	Perbix	Perbix	4/14/09	0	0	n/a
T1	4/29/09	Unknown	Cafiero	Cafiero	4/29/09	0	0	n/a
T10	5/13/09	O'Brien	Perbix	Perbix	5/14/09	0	0	124
T5	12/9/09	O'Brien	Perbix	Perbix	12/9/09	0	0	178
TOTAL						**5**	**5**	

H. Nature of Images Recovered

We reviewed the One-to-One laptop webcam photographs recovered in the investigation for the nature of their content. Because the photographs captured whatever was in front of the laptop at a given moment, a number of them show walls or empty or dark rooms with no people. Many others were taken while the student was in school and show students in classrooms. There are, however, many photographs of students and family members or other individuals in their homes and elsewhere. While such photographs are inherently troubling, we think it is important to note that none of the photographs contains nudity.[129]

We also reviewed generally the One-to-One laptop screenshots recovered in the investigation. Because the screenshots depict whatever was on the laptop's screen at a given moment, some include nothing but the laptop's "wallpaper," while others include, among other

[129] In an interview aired on "Good Morning America" on April 17, 2010, Blake J. Robbins, speaking about the webcam photographs captured from his laptop and referring to Ms. Matsko, said, "she's seen me naked."

Among all of the webcam photographs recovered in the investigation there are a number of photographs of males without shirts, and other content that the individuals appearing in the photographs might consider to be of a similarly personal nature. None of the photographs contains what would commonly be considered "nakedness."

things, images of schoolwork, websites, e-mails, and/or instant message conversations. Except with respect to the screenshots that are at issue in the Robbins litigation, we were not charged with reviewing or analyzing the student-created content contained in the screenshots – for example, we did not evaluate the content of e-mails or instant messages.

As noted above (at p. 8 n.14), a court order prohibits the District from disseminating any of the images without prior approval of the court, and United States Chief Magistrate Judge Thomas J. Rueter will oversee a process pursuant to which students and/or their families will be: (i) notified if the investigation has recovered any images captured by LANrev from those students' laptops; and (ii) provided an opportunity to view any such images.

I. IS Personnel Periodically Purged Images from the LANrev Server To Improve LANrev's Performance

The District's Records Management Policy, adopted in October 2007, outlines general guidelines but provides that "[t]he Superintendent or the Superintendent's designee shall work with appropriate administrative staff and the District's Solicitor to develop such Administrative Regulations which are necessary and appropriate to ensure compliance with applicable federal and state laws and regulations."[130] No such regulations have been promulgated. In addition, the IS Department had no specific policy governing the retention of data stored on the LANrev inventory server, which held the images and other data collected via TheftTrack. And, as was the case with the implementation of TheftTrack, no one raised this issue with the District solicitor.

Mr. Perbix purged the TheftTrack data from the LANrev inventory server on March 12, 2009 after discovering that the large volume of tracking data had hampered LANrev's

[130] LMSD Policy No. 800, Records Management, App. Tab 11.

performance.[131] The purged data included the IP-only tracking information collected from laptops for which insurance fees had not been paid, as well as the images and other tracking data collected from the six laptops that had been stolen from an HHS locker room in September 2008. Mr. Perbix found that LANrev's "performance [was] much snappier" as a result of the purge.[132]

As a matter of general practice after March 12, 2009, Mr. Perbix purged LANrev tracking data for particular laptops when TheftTrack was deactivated for those laptops. In addition, the IS department purged the inventory server in September 2009 for the beginning of the new school year.

L-3's report discusses the extensive forensic work that it did to recover much of the tracking data that had been purged from the LANrev inventory server. It also describes how Mr. Perbix took steps to preserve images and other tracking data on February 20, 2010 at the outset of the Robbins litigation.[133]

V. CONCLUSIONS AND RECOMMENDATIONS

LANrev TheftTrack provides organizations a means of remotely capturing webcam photographs and screenshots from their computers. The ostensible purpose of the technology is to assist in recovering stolen computers. The District used TheftTrack for that purpose, and indeed was successful in working with the police to recover stolen laptops.

[131] E-mail from M. Perbix to C. Cafiero, dated March 12, 2009, App. Tab 112.

[132] E-mails among M. Perbix and LANrev technical support staff, dated from March 6 through March 13, 2009, App. Tab 55; E-mail from M. Perbix to C. Cafiero, dated March 12, 2009, App. Tab 112.

[133] *See* L-3 Report at 17.

In the absence of policies and procedures governing its use, however – and without disclosing to students and their families the existence of TheftTrack's capabilities – the District also used TheftTrack to remotely capture images from:

- student laptops that were reported missing (as opposed to stolen);
- student laptops that were not returned by students who had withdrawn from school; and
- in one circumstance, a student laptop that was subject to unpaid insurance fees.

And, in a reflection of the District's deficient controls and recordkeeping, the District: (i) activated TheftTrack in additional instances for which the reason for activation cannot be determined; and (ii) allowed TheftTrack to remain activated – sometimes for long periods of time – in a number of instances in which there was no longer any possible legitimate reason for remotely capturing images from students' laptops. As a result, the District captured thousands of webcam photographs and screenshots from the laptops of unsuspecting students and other users.

Thus, although we found no evidence that District personnel used TheftTrack to "spy" on students, or that District personnel surreptitiously downloaded images from the LANrev server, our investigation leaves unresolved questions that raise serious concerns about why so many images were captured without apparent regard for privacy considerations.

Based upon our findings and conclusions, we recommend that the District:

- Adopt as soon as practicable an official policy prohibiting the remote activation of webcams on computers issued to students;
- Adopt as soon as practicable an official policy prohibiting the remote capturing of screenshots from computers issued to students (except to the extent that may be permitted by official policies and procedures governing the manner and circumstances in which District personnel may remotely access computers issued to students or review any data contained on computers issued to students);
- Consider implementing a cost-effective, technological alternative to image-based tracking to track lost or missing computers, so long as the alternative: (i) is used for security purposes only, (ii) operates in a manner that would not compromise

the privacy rights of District students or their families, and (iii) is disclosed to students and their families;

- Refrain from purchasing any software, hardware, or other technology that allows for the remote activation of webcams (except to the extent any standard operating system software or other commercially available software that the District may wish to use for educational purposes includes functionality that could possibly allow for the remote activation of webcams, in which case the District should, to the extent feasible, disable any such functionality);

- Adopt no later than the beginning of the 2010-2011 school year official policies and procedures:

    - governing the distribution, maintenance, and use of student computers;

    - addressing the privacy of student data with respect to student computers; and

    - requiring the training of administrators, teachers, and Information Services Department personnel with respect to student laptops and privacy.

    Such policies should require, among other things:

    - that the District explain to, and obtain the consent of, parents, guardians, and students with respect to, the manner and circumstances in which District personnel may remotely access student computers or access or review any information or data (including but not limited to documents, e-mails, instant messaging, photographs, Internet usage logs, and Web browsing histories) contained on student computers; and

    - the Information Services Department to maintain a permanent log of each and every instance in which it remotely accesses any student computers that details the date and time of remote access and the reason for such access;

- Continue to work with United States Magistrate Judge Thomas J. Rueter to develop a process pursuant to which students and/or their families will be:

    - notified if the investigation has recovered any images captured by LANrev from those students' laptops; and

    - provided an opportunity to view any such images;

- Ensure that all images captured via the LANrev TheftTrack feature that are in the possession of the District or its agents are permanently destroyed promptly after the foregoing process and any litigation or governmental investigation that requires the preservation of such images has concluded; and

- Promulgate as soon as practicable regulations pursuant to its Records Management Policy that address, among other things, the retention of electronic data, including electronic data related to student laptops.