CINDY COHN (SBN 145997)
cindy@eff.org
LEE TIEN (SBN 148216)
KURT OPSAHL (SBN 191303)
JAMES S. TYRE (SBN 083117)
MARK RUMOLD (SBN 279060)
ANDREW CROCKER (SBN 291596)
DAVID GREENE (SBN 160107)
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Fax: (415) 436-9993

RICHARD R. WIEBE (SBN 121156)
wiebe@pacbell.net
LAW OFFICE OF RICHARD R. WIEBE
One California Street, Suite 900
San Francisco, CA 94111
Telephone: (415) 433-3200
Fax: (415) 433-6382

RACHAEL E. MENY (SBN 178514)
rmeny@kvn.com
BENJAMIN W. BERKOWITZ (SBN 244441)
MICHAEL S. KWUN (SBN 198945)
AUDREY WALTON-HADLOCK (SBN 250574)
JUSTINA K. SESSIONS (SBN 270914)
PHILIP J. TASSIN (SBN 287787)
KEKER & VAN NEST, LLP
633 Battery Street
San Francisco, CA 94111
Telephone: (415) 391-5400
Fax: (415) 397-7188

THOMAS E. MOORE III (SBN 115107)
tmoore@rroyselaw.com
ROYSE LAW FIRM, PC
1717 Embarcadero Road
Palo Alto, CA 94303
Telephone: (650) 813-9700
Fax: (650) 813-9777

ARAM ANTARAMIAN (SBN 239070)
aram@eff.org
LAW OFFICE OF ARAM ANTARAMIAN
1714 Blake Street
Berkeley, CA 94703
Telephone: (510) 289-1626

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

CAROLYN JEWEL, TASH HEPTING, YOUNG BOON HICKS, as executrix of the estate of GREGORY HICKS, ERIK KNUTZEN and JOICE WALTON, on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

NATIONAL SECURITY AGENCY, *et al.*,

Defendants.

CASE NO. 08-CV-4373-JSW

OCTOBER 24, 2014 DECLARATION OF RICHARD R. WIEBE IN SUPPORT OF PLAINTIFFS' MOTION FOR PARTIAL SUMMARY JUDGMENT

(Fourth Amendment Violation)

Date: December 19, 2014
Time: 9:00 a.m.
Courtroom 5, Second Floor
The Honorable Jeffrey S. White

I, Richard R. Wiebe, do hereby declare:

1. I am a member in good standing of the Bar of the State of California and the bar of this Court. I am counsel to plaintiffs in this action. Except as otherwise stated below, I could and would testify competently to the following.

2. **Exhibit A:** Attached hereto as Exhibit A is a true and correct copy of pages 33-34 of the Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (July 2, 2014) ("PCLOB 702 Report"), *available at* http://www.pclob.gov/All Documents/Report on the Section 702 Program/PCLOB-Section-702-Report.pdf.

3. **Exhibit B:** Attached hereto as Exhibit B is a true and correct copy of AT&T Inc.'s transparency report for the first half of 2014, *available at* http://about.att.com/content/dam/csr/PDFs/ATT_Transparency%20Report_July%202014.pdf.

4. **Exhibit C:** Attached hereto as Exhibit C is a true and correct copy of an excerpt from the court reporter's transcript of the hearing held June 24, 2006 in the United States District Court for the Northern District of California before Chief District Judge Vaughn R. Walker in the related action of *Hepting v. AT&T*, No. 06-CV-0672-VRW.

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct to the best of my knowledge, information, and belief.

Executed at San Francisco, CA on October 24, 2014.

s/ *Richard R. Wiebe*
Richard R. Wiebe

EXHIBIT A

PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act

JULY 2, 2014

considered targets — and therefore only selectors used by non-U.S. persons reasonably believed to be located abroad may be tasked. The targeting procedures govern both the targeting and tasking process.

Because such terms would not identify specific communications facilities, selectors may not be key words (such as "bomb" or "attack"), or the names of targeted individuals ("Osama Bin Laden").[114] Under the NSA targeting procedures, if a U.S. person or a person located in the United States is determined to be a user of a selector, that selector may not be tasked to Section 702 acquisition or must be promptly detasked if the selector has already been tasked.[115]

Although targeting decisions must be individualized, this does not mean that a substantial number of persons are not targeted under the Section 702 program. The government estimates that 89,138 persons were targeted under Section 702 during 2013.[116]

Once a selector has been tasked under the targeting procedures, it is sent to an electronic communications service provider to begin acquisition. There are two types of Section 702 acquisition: what has been referred to as "PRISM" collection and "upstream" collection. PRISM collection is the easier of the two acquisition methods to understand.

B. PRISM Collection

In PRISM collection, the government (specifically, the FBI on behalf of the NSA) sends selectors — such as an email address — to a United States–based electronic communications service provider (such as an Internet service provider, or "ISP") that has been served a directive.[117] Under the directive, the service provider is compelled to give the communications sent to or from that selector to the government (but not communications that are only "about" the selector, as described below).[118] As of mid-2011, 91 percent of the

---

114 NSA DCLPO REPORT, *supra*, at 4; PCLOB March 2014 Hearing Transcript, *supra*, at 57 (statement of Rajesh De, General Counsel, NSA) (noting that a name cannot be tasked).

115 NSA DCLPO REPORT, *supra*, at 6.

116 OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE STATISTICAL TRANSPARENCY REPORT REGARDING USE OF NATIONAL SECURITY AUTHORITIES: ANNUAL STATISTICS FOR CALENDAR YEAR 2013, at 1 (June 26, 2014), a*vailable at* http://www.dni.gov/files/tp/National_Security_Authorities_Transparency_Report_CY2013.pdf. In calculating this estimate, the government counted two known people using one tasked email address as two targets and one person known to use two tasked email addresses as one target. The number of targets is an estimate because the government may not be aware of all of the users of a particular tasked selector.

117 The Intelligence Community's Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, *supra*, at 3. *See also* PCLOB March 2014 Hearing Transcript at 70 (statement of Rajesh De, General Counsel, NSA) (noting any recipient company "would have received legal process").

118 PCLOB March 2014 Hearing Transcript at 70; *see also* NSA DCLPO REPORT, *supra*, at 5.

Internet communications that the NSA acquired each year were obtained through PRISM collection.[119]

The government has not declassified the specific ISPs that have been served directives to undertake PRISM collection, but an example using a fake United States company ("USA-ISP Company") may clarify how PRISM collection works in practice: The NSA learns that John Target, a non-U.S. person located outside the United States, uses the email address "johntarget@usa-ISP.com" to communicate with associates about his efforts to engage in international terrorism. The NSA applies its targeting procedures (described below) and "tasks" johntarget@usa-ISP.com to Section 702 acquisition for the purpose of acquiring information about John Target's involvement in international terrorism. The FBI would then contact USA-ISP Company (a company that has previously been sent a Section 702 directive) and instruct USA-ISP Company to provide to the government all communications to or from email address johntarget@usa-ISP.com. The acquisition continues until the government "detasks" johntarget@usa-ISP.com.

The NSA receives all PRISM collection acquired under Section 702. In addition, a copy of the raw data acquired via PRISM collection — and, to date, only PRISM collection — may also be sent to the CIA and/or FBI.[120] The NSA, CIA, and FBI all must apply their own minimization procedures to any PRISM-acquired data.[121]

Before data is entered into systems available to trained analysts or agents, government technical personnel use technical systems to help verify that data sent by the provider is limited to the data requested by the government. To again use the John Target example above, if the NSA determined that johntarget@usa-ISP.com was not actually going to be used to communicate information about international terrorism, the government would send a detasking request to USA-ISP Company to stop further Section 702 collection on this email address. After passing on the detasking request to USA-ISP Company, the government would use its technical systems to block any further Section 702 acquisition from johntarget@usa-ISP.com to ensure that Section 702 collection against this address was immediately terminated.

---

119 Bates October 2011 Opinion, *supra*, at 29-30 and n.24, 2011 WL 10945618, at *25 & n.24.

120 Minimization Procedures used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended, § 6(c) (Oct. 31, 2011) ("NSA 2011 Minimization Procedures"), *available at* http://www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20SECT%20702.pdf.

121 NSA 2011 Minimization Procedures, *supra*, § 6(c).

EXHIBIT B

AT&T Transparency Report

Introduction

We take our responsibility to protect your information and privacy very seriously. We continue our pledge to protect your privacy to the fullest extent possible and in compliance with the laws of the country where your service is provided.

Like all companies, we are required by law to provide information to government and law enforcement agencies, as well as parties to civil lawsuits, by complying with court orders, subpoenas, lawful discovery requests and other legal requirements. We ensure that these requests are valid, and that our responses comply with the law and our own policies.

This Report

AT&T's first Transparency Report provided information for 2013. In fulfillment of our commitment to issue reports on a semiannual basis, this report provides specific information regarding the number and types of demands to which we responded from Jan. 1, 2014 through June 30, 2014, as well as National Security Demands for the second half of 2013 which we are providing subject to the U.S. Department of Justice's guidelines. This report doesn't include any numbers or information for Cricket™ Wireless because they weren't acquired until March 2014. We plan to include Cricket's data in our next report.

What's New?

We appreciate the comments we received on AT&T's first Transparency Report. We have incorporated changes to provide you with more transparency. These changes include:

- Disclosing the specific number of wiretaps, pen registers, and general court orders processed.
- A clearer statement that we require a search warrant or probable cause order before providing any stored content.

The chart below includes hyperlinks to additional information on the category of data reported.

NATIONAL SECURITY DEMANDS

National Security Letters (Jan. 1 – June 30, 2014)	
▪ Total Received	1,000-1,999
▪ Number of Customer Accounts	2,000-2,999
Foreign Intelligence Surveillance Act (July 1 – Dec. 31, 2013) [1]	
▪ Total Content	0-999
○ Customer Accounts	33,000-33,999
▪ Total Non-Content	0-999
○ Customer Accounts	0-999

TOTAL U.S. CRIMINAL & CIVIL LITIGATION DEMANDS

Total Demands (Federal, State and Local; Criminal and Civil)			**115,925**
▪ Subpoenas		**86,943**	
○ Criminal	78,975		
○ Civil	7,968		
▪ Court Orders (General)		**15,105**	
○ Historic	12,569		
○ Real-time (Pen registers)	2,536	**9,393**	
▪ Search Warrants/Probable Cause Court Orders			
○ Historic			
▪ Stored Content	2,532		
▪ All Others	6,861		
○ Real-Time		**4,484**	
▪ Wiretaps	1,167		
▪ Mobile Locate Demands	3,317		

[1] The Department of Justice imposes a six-month delay for reporting this data.

DEMANDS REJECTED/PARTIAL OR NO DATA PROVIDED

(Breakout detail of data included in Total U.S. Criminal & Civil Litigation)

Total		**31,097**
▪ Rejected/Challenged	2,110	
▪ Partial or No Information	28,987	

LOCATION DEMANDS

(Breakout detail of data included in Total U.S. Criminal & Civil Litigation)

Total		**30,886**
▪ Historical	23,646	
▪ Real-time	6,956	
▪ Cell Tower Searches	284	

EMERGENCY REQUESTS

Total		**50,232**
▪ 911	39,449	
▪ Exigent	10,783	

INTERNATIONAL DEMANDS

Total Demands		**17**
▪ Law Enforcement	11	
▪ URL/IP Blocking	6	

Explanatory Notes

NATIONAL SECURITY DEMANDS

The Department of Justice's guidance, issued on Jan. 27, 2014, authorized us to report on the receipt of National Security Letters and court orders issued under the Foreign Intelligence Surveillance Act (FISA), with the exception of data, if any, related to the so-called bulk telephony metadata program. *See* http://www.justice.gov/opa/pr/2014/January/14-ag-081.html.

National Security Letters are subpoenas issued by the Federal Bureau of Investigation in regard to counterterrorism or counterintelligence. These subpoenas are limited to non-content information, such as a list of phone numbers dialed or subscriber information.

Court orders issued pursuant to FISA may direct us to respond to government requests for content and non-content data related to national security investigations, such as international terrorism or espionage.

These types of demands have very strict policies governing our ability to disclose the requests. The recent "Statistical Transparency Report Regarding Use of National Security Authorities" published by the Director of National Intelligence on June 26, 2014, does not alter the Department of Justice's Jan. 27, 2014, guidance.
See http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2013.

Consistent with guidance from January 2014, our report includes the range of customer accounts potentially impacted by these National Security Demands.

TOTAL U.S. CRIMINAL & CIVIL LITIGATION DEMANDS

This number includes demands to which we responded in connection with criminal and civil litigation matters. This category doesn't include demands reported in our National Security Demands table.

Criminal proceedings include actions by the government — federal, state, and local — against an individual arising from an alleged violation of applicable criminal law.

Civil actions include lawsuits involving private parties (i.e., a personal liability case, divorce proceeding, or any type of dispute between private companies or individuals). In addition, civil proceedings include investigations by governmental regulatory agencies such as the Securities and Exchange Commission, the Federal Trade Commission and the Federal Communications Commission.

We ensure we receive the right type of legal demand.

We receive several types of legal demands, including subpoenas, court orders, and search warrants. Before we respond to **any** legal demand, we determine that we have received the correct type of demand based on the applicable federal and state laws and the type of information being sought. For instance, in some states we must supply call detail records if we receive a subpoena. In other states, call detail records require a court order or search warrant. If the requesting agent has failed to send the correct type of demand, we reject the demand.

Types of Legal Demands

Subpoenas, court orders and search warrants are used to demand information for use in criminal trials, lawsuits, investigations, and other proceedings. If the applicable rules are followed, we're legally required to provide the information.

In this, our second report, we have changed the reporting for "Total U.S. Criminal & Civil Demands" to more accurately reflect the type of demand with the information requested, particularly relating to general court orders and search warrants.

- **Subpoenas** don't usually require the approval of a judge and are issued by an officer of the court. They are used in both criminal and civil cases, typically to obtain written business documents such as calling records.

- **General Court Orders** are signed by a judge. We consider "general" court orders as all orders except those that contain a probable cause finding. In a criminal case, for example, a judge may issue a court order on a lesser standard than probable cause, such as "relevant to an ongoing criminal investigation." In a civil case, a court order may be issued on a "relevant" or "reasonably calculated to lead to the discovery of admissible evidence" standard. For this report, general court orders were used to obtain historical information like billing records or the past location of a wireless device. In criminal cases, they are also used to obtain real-time, pen register/"trap and trace" information, which provides phone numbers and other dialed information for all calls as they are made or received from the device identified in the order.

- **Search Warrants and Probable Cause Court Orders** are signed by a judge, and they are issued only upon a finding of "probable cause." To be issued, the warrant or order must be supported by sworn testimony and sufficient evidence to believe the information requested is evidence of a crime. Probable cause is viewed as the highest standard to obtain evidence. Except in emergency circumstances, a search warrant or probable cause court order for all real-time location information (i.e., wiretaps and GPS) and stored

content (i.e., text and voice messages) is required for all jurisdictions, courts, and agencies.

DEMANDS REJECTED/PARTIAL OR NO DATA PROVIDED

We ensure that we receive the appropriate type of demand for the information requested. In this category, we include the number of times we rejected a demand or provided only partial information or no information in response to a demand. Here are a few reasons why certain demands fall into this category:

- The wrong type of demand is submitted by law enforcement. For instance, we will reject a subpoena requesting a wiretap, because either a probable cause court order or search warrant is required.
- The demand has errors, such as missing pages or signatures.
- The demand was not correctly addressed to AT&T.
- The demand did not contain all of the elements necessary for a response.
- We had no information that matched the customer or equipment information provided in the demand.

LOCATION DEMANDS

Our Location Demands category breaks out the number of court orders and search warrants we received by the type of location information (historical and real-time) they requested. We also provide the number of requests we received for cell tower searches, which ask us to provide all telephone numbers registered to a particular cell tower for a certain period of time (or to confirm whether a particular telephone number registered on a particular cell tower at a given time). We do not keep track of the number of telephone numbers provided to law enforcement in connection with cell tower searches.

A single cell tower demand may cover multiple towers. In our last report, we disclosed the total number of cell tower searches. For clarity, we are now disclosing the total numbers of demands and the total number of searches. For instance, if we received one court order that included ID numbers for two cell towers, we count that as one demand for two searches. For the 284 cell tower demands during this period, we performed 708 searches. We also maintain a record of the average time period that law enforcement requests for one cell tower search, which was 2 hours, 23 minutes for this reporting period.

Except in emergency situations, we require the most stringent legal standard — a search warrant or probable cause court order — for all demands for specific location information. The legal standard required for the production of other location data is unsettled. Some courts have

decided that a general court order is sufficient legal process for law enforcement to obtain such location data. Other courts have determined that the Fourth Amendment requires law enforcement to first obtain a search warrant or probable cause court order before seeking this location information. With the exception of emergency situations, we require an order signed by a judge before producing any type of location information to law enforcement. We will continue to follow these legal developments and, in all circumstances, we will comply with the applicable law.

EMERGENCY REQUESTS

This category includes the number of times we responded to 911-related inquiries and "exigent requests" to help locate or identify a 911 caller. These are emergency requests from law enforcement working on kidnappings, missing person cases, attempted suicides and other emergencies. The numbers provided in this category are the total of 911 and exigent searches that we processed during this reporting period.

Even when responding to an emergency, we protect your privacy:

- When responding to 911 inquiries, we confirm the request is coming from a legitimate Public Safety Answering Point before quickly responding.
- For exigent requests, we receive a certification from a law enforcement agency confirming they are dealing with a case involving risk of death or serious injury before we share information.

INTERNATIONAL DEMANDS

International Demands represent the number of demands we received from governments outside the U.S., and relate to AT&T's global business operations in these countries. Such International Demands are for customer information stored in their countries, and URL/IP (website/Internet address) blocking requests.

We are not a content provider outside the U.S. but are required by some countries' laws to comply with requests to block access to websites that are deemed offensive, illegal, unauthorized or otherwise inappropriate in certain countries. These requests might be designed to block sites related to displaying child pornography, unregistered and illegal gambling, defamation, illegal sale of medicinal products, or trademark and copyright infringement. A demand may request that one or more identifiers (i.e., IP addresses or URLs) be blocked.

The majority of law enforcement demands involve requests for information relating to individuals. Because our global operations support only very large multi-national business customers, we received relatively few international demands. We do not have a mobility network outside the U.S., and we don't provide services to individual consumers residing outside the U.S. We received no demands from the U.S. government for data stored outside the U.S. If we receive an international demand for information stored in the U.S., we refer it to that country's Mutual Legal Assistance Treaty (MLAT) process. The Federal Bureau of Investigation ensures that we receive the proper form of U.S. process (e.g., subpoena, court order or search warrant), subject to the

limitations placed on discovery in the U.S., and that cross-border data flows are handled appropriately. Thus, any international-originated demands that follow an MLAT procedure are reported in our Total Demands category because we can't separate them from any other Federal Bureau of Investigation demand we may receive.

ADDITIONAL RESOURCES

You'll find more on our commitment to privacy in:

- Our Privacy Policy.
- Our issues brief on Privacy.
- Our issues brief on Freedom of Expression.

EXHIBIT C

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

BEFORE THE HONORABLE VAUGHN R. WALKER, JUDGE

TASH HEPTING, et al.,

Plaintiffs,

v. **06 C 0672 VRW**

AT&T Corp., et al.,

Defendants.

San Francisco, CA
June 23, 2006
9:40 a.m.

Pages 1 - 121

TRANSCRIPT OF PROCEEDINGS

APPEARANCES:

HELLER, EHRMAN, LLP
Attorneys for Plaintiffs
BY: ROBERT D. FRAM
NATHAN E. SHAFROTH
ELENA DiMUZIO

ELECTRONIC FRONTIER FOUNDATION
Attorneys for Plaintiffs
BY: CINDY COHN
KEVIN S. BANKSTON
KURT OPSAHL
LEE TIEN

LERACH, COUGHLIN, STOIA, GELLER, RUDMAN & ROBBINS, LLP
Attorneys for Plaintiffs
BY: JEFF D. FRIEDMAN
MARIA V. MORRIS
REED R. KATHREIN

RICHARD R. WIEBE
Attorney for Plaintiffs

CONNIE KUHL, RMR, CRR
Official Reporter - U.S. District Court (415) 431-2020

APPEARANCES (cont.):

THE UNITED STATES OF AMERICA, DOJ
The Office of the Attorney General
BY: PETER D. KEISLER, Assistant Attorney General
CARL J. NICHOLS, Deputy Assistant Attorney General
JOSEPH HUNT

PILLSBURY, WINTHROP, SHAW & PITTMAN, LLP
Attorneys for Defendants AT&T Corp., et al.
BY: BRUCE A. ERICSON
DAVID L. ANDERSON
JACOB R. SORENSEN

SIDLEY, AUSTIN, LLP
Attorneys for Defendants AT&T Corp., et al.
BY: BRADFORD A. BERENSON

LEVY, RAM & OLSON, LLP
Attorneys for Intervenors The San Francisco Chronicle, LA Times, San Jose Mercury News, Bloomberg News, Associated Press
BY: KARL OLSON

QUINN EMANUEL
Attorneys for Intervenors Lycos and Wired News
BY: TIMOTHY L. ALGER

Reported By: Connie Kuhl, RMR, CRR
Official Court Reporter

Friday, June 23rd, 2006

9:40 a.m.

DEPUTY CLERK: Calling civil Case 06-0672, Tash Hepting, et al. versus AT&T Corporation, et al.

Counsel, state your appearances, please.

MR. FRAM: Robert Fram, Heller, Ehrman, for the plaintiffs, your Honor.

THE COURT: Good morning.

MR. BANKSTON: Kevin S. Bankston, Electronic Frontier Foundation for the plaintiffs, your Honor.

THE COURT: Good morning, sir.

MS. COHN: Cindy Cohn, Electronic Frontier Foundation, for the plaintiffs, your Honor.

THE COURT: Miss Cohn, good morning.

MR. TYRE: James Tyre, also for plaintiffs.

THE COURT: Good morning, Mr. Tyre.

MR. WIEBE: Richard Wiebe for the plaintiffs.

MR. OPSAHL: Kurt Opsahl, also for the plaintiffs.

MR. TIEN: Lee Tien for the plaintiffs.

MR. FRIEDMAN: Jeff Friedman, Lerach, Coughlin, for the plaintiffs.

THE COURT: Is that it?

MR. BERENSON: Bruce Berenson from Sidley, Austin, for Defendants AT&T.

THE COURT: Good morning.

one and two. I don't know if you want that now or reserve that --

THE COURT: Why don't we use that in any wrap-up we have, any wrap-up discussion. All right?

MR. FRAM: Thank you, your Honor.

THE COURT: Thank you, Mr. Fram.

Very quickly, Mr. Keisler? It is Keisler?

MR. KEISLER: It is, your Honor.

First of all, with respect to the suggestion that the plaintiffs already put forward a prima facie case. They note correctly that we haven't said any documents are classified. They say we can't now unring that bell. We don't want to unring that bell. None of the documents they have submitted to accompany these declarations implicate any privileged matters.

THE COURT: Including the Klein documents.

MR. KEISLER: We have not asserted any privilege over the information that is in the Klein and Marcus declarations.

THE COURT: Either in the declaration or its exhibits?

MR. KEISLER: We have not asserted a privilege over either of those. Mr. Klein and Marcus never had access to any of the relevant classified information here, and with all respect to them, through no fault or failure of their own, they don't know anything. And that's clear from the face of the declarations. And since Mr. Fram talked about them some, I may respond on that.

The plaintiffs rely on Mr. Klein's declaration of the asserted connection between AT&T and the NSA. Absolutely every assertion he makes in his declaration about that relationship is hearsay. It's one person told me that a third person who briefly visited the AT&T offices was from the NSA. And the statement that Mr. Fram quoted --

THE COURT: It has to be admissible in the summary judgment stage; we're not there yet.

MR. KEISLER: I'm just addressing whether they have a prima facie case, which I understand would be a case if the Court could issue a judgment, if it were unrebutted.

THE COURT: The absence of a rebuttal.

MR. KEISLER: And saying to my knowledge no one was permitted in a particular AT&T room who was not cleared by the NSA without giving any basis, not even a hearsay basis, for that claim of knowledge, would not be an element even of a prima facie case.

And with respect to Mr. Marcus, he acknowledges that he doesn't actually know even what equipment is in any room at AT&T. He's reading from a document, and all he testifies to as to what he understands are the capabilities of that equipment to be, and he says those capabilities are consistent with what he's read in the newspapers. But he doesn't know whether those pieces of equipment, if they're there, are actually used for those capabilities. And he acknowledges that that equipment

also has what he calls other legitimate possible uses. So the notion that this mixture of hearsay and speculation could be a prima facie case sufficient to sustain a judgment in the absence of rebuttal we think is just wrong.

But even if they had a more robust case, even if they had a real prima facie case, your Honor would run exactly into the portion of *Kasza* which your Honor quoted which is that even if plaintiffs can bring forward some non privileged evidence, if the very subject of the action is a state secret or if state secrets would prevent the defendant from producing important information in its defense, then judgment can be entered.

THE COURT: Isn't this case different, though? Different from the *Kasza* case? After all, *Kasza* dealt with a situation in which the whole program of disposing of these materials at the Grooms Lake facility or wherever it was, was involved and could not litigate the case without getting into that entire program disposal, and indeed it was the program of disposal that was the state secret. So the state secret was coextensive with all the evidence necessary for a plaintiff to proceed in that case, and it's not our case here, is it.

MR. KEISLER: We think it's exactly the case. The *Kasza* case said, no procedures can be at suit because classified information is an essential element of every one of the claims. We think that is precisely the case here.

Obviously they can't prove liability against AT&T