



UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549

DIVISION OF
CORPORATION FINANCE

February 20, 2014

Wayne A. Wirtz
AT&T Inc.
ww0118@att.com

Re: AT&T Inc.

Dear Mr. Wirtz:

This is in regard to your letter dated February 20, 2014 concerning the shareholder proposal submitted by the New York State Common Retirement Fund; Trillium Asset Management LLC on behalf of Louise Rice; Harrington Investments, Inc. on behalf of Sarah Nelson; and Arjuna Capital/Baldwin Brothers Inc. on behalf of Tamara Davis, John Silva and Shana Weiss for inclusion in AT&T's proxy materials for its upcoming annual meeting of security holders. Your letter indicates that the proponents have withdrawn the proposal and that AT&T therefore withdraws its December 5, 2013 request for a no-action letter from the Division. Because the matter is now moot, we will have no further comment.

Copies of all of the correspondence related to this matter will be made available on our website at <http://www.sec.gov/divisions/corpfin/cf-noaction/14a-8.shtml>. For your reference, a brief discussion of the Division's informal procedures regarding shareholder proposals is also available at the same website address.

Sincerely,

Evan S. Jacobson
Special Counsel

cc: Sanford Lewis
sanfordlewis@gmail.com



Wayne A. Wirtz
AT&T Inc.
Associate General Counsel
208 S. Akard, Room 3024
Dallas, Texas 75202
(214) 757-3344
ww0118@att.com

1934 Act/Rule 14a-8

By email to shareholderproposals@sec.gov

February 20, 2014

U.S. Securities and Exchange Commission
Division of Corporation Finance
Office of Chief Counsel
100 F St., NE
Washington, DC 20549

Re: AT&T Inc. – Request to Exclude Shareholder Proposal of the New York State
Common Retirement Fund et al.

Ladies and Gentlemen:

We have received correspondence from the New York State Common Retirement Fund indicating they have withdrawn the above proposal on behalf of all proponents. As requested, attached is correspondence from the proponent. AT&T no longer seeks a “no-action” response from the staff.

Sincerely,

A handwritten signature in black ink, appearing to read "W. Wirtz".

Wayne Wirtz

WIRTZ, WAYNE A (Legal)

From: PDoherty@osc.state.ny.us
Sent: Wednesday, February 19, 2014 2:43 PM
To: WIRTZ, WAYNE A (Legal)
Subject: RE: Withdrawal of NYS Resolution

Yes, we withdrew on behalf of New York State as the lead filer and also on behalf of the co-filers.
- Patrick Doherty

Patrick Doherty
Director - Corporate Governance
Office of the State Comptroller
633 Third Avenue, 31st Floor
New York, New York 10017-6754
212.681.4823 (Tel.)
212.681.4468 (Fax)

From: "WIRTZ, WAYNE A (Legal)" <ww0118@att.com>
To: "PDoherty@osc.state.ny.us" <PDoherty@osc.state.ny.us>,
Date: 02/19/2014 03:09 PM
Subject: RE: Withdrawal of NYS Resolution

So, are you withdrawing on behalf of your co-sponsors? Your letter was pretty specific that only the NY Controller was withdrawing.

From: PDoherty@osc.state.ny.us [mailto:PDoherty@osc.state.ny.us]
Sent: Wednesday, February 19, 2014 2:08 PM
To: WIRTZ, WAYNE A (Legal)
Subject: Fw: Withdrawal of NYS Resolution

Mr. Wirtz -
The filing letters of the co-sponsors explicitly authorize us as lead filer to act on their behalf in this regard.
- Patrick Doherty

Patrick Doherty
Director - Corporate Governance
Office of the State Comptroller
633 Third Avenue, 31st Floor
New York, New York 10017-6754
212.681.4823 (Tel.)
212.681.4468 (Fax)

----- Forwarded by Patrick Doherty/ICM/NYSOSC on 02/19/2014 03:06 PM -----

From: "WIRTZ, WAYNE A (Legal)" <ww0118@att.com>
To: "PDoherty@osc.state.ny.us" <PDoherty@osc.state.ny.us>,
Cc: "MSweeney@osc.state.ny.us" <MSweeney@osc.state.ny.us>
Date: 02/19/2014 03:05 PM
Subject: RE: Withdrawal of NYS Resolution

Thank you for correspondence. I was disappointed to see that only the NY fund was withdrawing the proposal.

From: PDoherty@osc.state.ny.us [mailto:PDoherty@osc.state.ny.us]
Sent: Wednesday, February 19, 2014 1:53 PM
To: WIRTZ, WAYNE A (Legal)
Cc: MSweeney@osc.state.ny.us
Subject: Withdrawal of NYS Resolution

Mr. Wirtz -
Please see attached letter withdrawing our shareholder proposal.
- Patrick Doherty

Patrick Doherty
Director - Corporate Governance
Office of the State Comptroller
633 Third Avenue, 31st Floor
New York, New York 10017-6754
212.681.4823 (Tel.)
212.681.4468 (Fax)

Notice: This communication, including any attachments, is intended solely for the use of the individual or entity to which it is addressed. This communication may contain information that is protected from disclosure under State and/or Federal law. Please notify the sender immediately if you have received this communication in error and delete this email from your system. If you are not the intended recipient, you are requested not to disclose, copy, distribute or take any action in reliance on the contents of this information.

Notice: This communication, including any attachments, is intended solely for the use of the individual or entity to which it is addressed. This communication may contain information that is protected from disclosure under State and/or Federal law. Please notify the sender immediately if you have received this communication in error and delete this email from your system. If you are not the intended recipient, you are requested not to disclose, copy, distribute or take any action in reliance on the contents of this information.

Notice: This communication, including any attachments, is intended solely for the use of the individual or entity to which it is addressed. This communication may contain information that is protected from disclosure under State and/or Federal law. Please notify the sender immediately if you have received this communication in error and delete this email from your system. If you are not the intended recipient, you are requested not to disclose, copy, distribute or take any action in reliance on the contents of this information.

THOMAS P. DINAPOLI
STATE COMPTROLLER



STATE OF NEW YORK
OFFICE OF THE STATE COMPTROLLER

PENSION INVESTMENTS
& CASI MANAGEMENT
633 Third Avenue-31st Floor
New York, NY 10017
Tel: (212) 681-4489
Fax: (212) 681-4468

February 19, 2014

Mr. Wayne Wirtz
AT&T Inc.
Associate General Counsel
208 South Akard
Dallas, Texas 75202

Dear Mr. Wirtz:

On the basis of your company's issuance of a "transparency report" containing information relating to government requests for customer information, I hereby withdraw the resolution filed with your company by the Office of the State Comptroller on behalf of the New York State Common Retirement Fund.

Very truly yours,

A handwritten signature in dark ink, appearing to read 'Patrick Doherty', written over a horizontal line.

Patrick Doherty
pd:jm
Enclosures



Wayne A. Wirtz
Associate General Counsel
Legal Department
208 S. Akard, Room 3024
Dallas, Texas 75202
(214) 757-3344
ww0118@att.com

1934 Act/Rule 14a-8

By email to shareholderproposals@sec.gov

February 17, 2014

U.S. Securities and Exchange Commission
Division of Corporation Finance
Office of Chief Counsel
100 F St., NE
Washington, DC 20549

Re: AT&T Inc. – Third Supplemental Request to Exclude Shareholder Proposal of the New York State Common Retirement Fund et al.

Ladies and Gentlemen:

The New York State Common Retirement Fund and co-filers Sarah Nelson, Louise Rice, Tamara Davis, John Silva and Shana Weiss (collectively, the “Proponents”) submitted a shareholder proposal (the “Proposal”) and statement in support thereof (the “Supporting Statement”) to AT&T Inc., a Delaware corporation (“AT&T” or the “Company”), for inclusion in AT&T’s proxy statement and form of proxy for its 2014 Annual Meeting of Shareholders (collectively, the “2014 Proxy Materials”). The Proposal requests that the Company “publish semi-annual reports, subject to existing laws and regulations, providing metrics and discussion regarding requests for customer information by U.S. and foreign governments, at reasonable cost and omitting proprietary information.”

This supplement is submitted in response to a letter from Sanford J. Lewis, counsel to the Proponents, dated January 24, 2014 (the “January 24 Response”), and in light of the February 17, 2014, publication of AT&T’s Transparency Report (“Transparency Report” or “Report”), which addresses civil and criminal process, National Security Letters (“NSLs”) and national security orders to the extent permitted by law and on par with the transparency reports of Internet companies. AT&T’s Transparency Report, a copy of which is attached to this request, is available on our website at <http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport.html>.

AT&T's publication of its Transparency Report and its commitment to publish additional Reports on a semi-annual basis substantially implement the Proposal, and we respectfully request that the Staff concur that it will take no action if the Company excludes the Proposal from its 2014 Proxy Materials pursuant to Exchange Act Rule 14a-8(i)(10).

BACKGROUND

On December 5, 2013, AT&T submitted a letter to the Staff stating its intent to exclude the Proposal from its 2014 Proxy Materials on the basis that, among other things, the Proposal relates to ordinary business matters.

On December 20, 2013, AT&T issued a press release announcing its intent to publish a Transparency Report disclosing law enforcement requests for customer information that AT&T received in 2013 in the United States and the other countries in which it does business. In light of this announcement, on December 27, 2013, AT&T supplemented its December 5, 2013 letter with a letter to the Staff adding a separate argument to exclude the Proposal pursuant to Rule 14a-8(i)(10) – substantial implementation.

On January 6, 2014, Mr. Lewis submitted a lengthy response to the Company's December 5 and December 27 letters (the "January 6 Response"). The January 6 Response asserts that the AT&T Transparency Report "would reflect only a small fragment of the disclosure required by the Proposal" and would not substantially implement the Proposal because "disclosures related to meta-data sharing with the NSA and any similar programs...would be excluded." The January 6 Response goes on to state, **"The current Proposal is essentially a request to AT&T to engage in reporting on par with the transparency reports of the internet companies"** (emphasis in original).

On January 20, 2014, the Company submitted a reply to the January 6 Response, arguing, among other things, that (i) the apparent request in the January 6 Response to disclose information regarding alleged intelligence communications, if implemented, would cause the Company to violate a series of federal laws and therefore could be excluded pursuant to Exchange Act Rule 14a-8(i)(2), and (ii) the January 6 Response both requests that the Company "engage in reporting on par with the transparency reports of the internet companies" and yet rejects as inadequate the Company's Transparency Report, which in fact would mirror those of the Internet companies, thereby rendering the Proposal vague and misleading and therefore excludable under Exchange Act Rule 14a-8(i)(3).

Mr. Lewis's January 24 Response seeks to clarify his January 6 Response by emphasizing that (i) the Proposal does not contemplate that AT&T should disclose any information it is not lawfully permitted to disclose, and (ii) the meaning of "reporting on par with" Internet companies was intended to reflect that such companies have, with the permission of the federal government, included in their transparency reports information related to the sharing of customer information in response to national security process "in an aggregated format," i.e., by providing "a number representing a range of National Security Letters received" during the reporting period.

On January 27, 2014, the Department of Justice provided new guidance¹ on two permissible methods by which communications providers could disclose information about the orders that they have received from the government: “Option One”² and “Option Two.”³

On February 17, 2014, AT&T published its first Transparency Report, which follows the Department of Justice’s “Option One.”

ARGUMENT

The Proposal May Be Excluded Pursuant to Exchange Act Rule 14a-8(i)(10) Because the Proposal Has Been Substantially Implemented.

Rule 14a-8(i)(10) permits a company to exclude a proposal from its proxy materials if the company “has already substantially implemented the proposal.” For a proposal to have been acted upon favorably by management, it is not necessary that the proposal have been implemented in full or precisely as presented. *See* Release No. 34-20091 (Aug. 16, 1983). Instead, “a determination that the company has substantially implemented the proposal depends upon whether [the company’s] particular policies practices and procedures compare favorably with the guidelines of the proposal.” *Texaco, Inc.* (Mar. 28, 1991). The general policy underlying the basis for exclusion under Rule 14a-8(i)(10) is “to avoid the possibility of shareholders having to consider matters which have already been favorably acted upon by the management.” Release No. 34-12598 (July 7, 1976).

The Proposal requests that the Company “publish semi-annual reports, subject to existing laws and regulations, providing metrics and discussion regarding requests for customer information by U.S. and foreign governments, at reasonable cost and omitting proprietary information.” The Supporting Statement provides that “[t]he reports should be prepared with consideration of existing Transparency (or Law Enforcement Request) Reports published by the

¹ *See* Letter from James M. Cole, Deputy Attorney General, U.S. Department of Justice, to Colin Stretch, Esq., Vice President and General Counsel, Facebook, et al., Jan. 27, 2014, available at <http://www.justice.gov/iso/opa/resources/366201412716018407143.pdf>.

² *Id.* Under “Option One,” communications providers may report aggregate data in the following separate categories: “1. Criminal process, subject to no restrictions. 2. The number of NSLs received, reported in bands of 1000 starting with 0-999. 3. The number of customer accounts affected by NSLs, reported in bands of 1000 starting with 0-999. 4. The number of [Foreign Intelligence Surveillance Act (“FISA”)] orders for content, reported in bands of 1000 starting with 0-999. 5. The number of customer selectors targeted under FISA content orders, in bands of 1000 starting with 0-999. 6. The number of FISA orders for non-content, reported in bands of 1000 starting with 0-999. 7. The number of customer selectors targeted under FISA non-content orders, in bands of 1000 starting with 0-999. A provider may publish the FISA and NSL numbers every six months. For FISA information, there will be a six-month delay between the publication date and the period covered by the report. For example, a report published on July 1, 2015, will reflect the FISA data for the period ending December 31, 2014.”

³ *Id.* Under “Option Two,” communications providers may report aggregate data in the following separate categories: “1. Criminal process, subject to no restrictions. 2. The total number of all national security process received, including all NSLs and FISA orders, reported as a single number in the following bands: 0-249 and thereafter in bands of 250. 3. The total number of customer selectors targeted under all national security process, including all NSLs and FISA orders, reported as a single number in the following bands, 0-249, and thereafter in bands of 250.”

major internet companies, and where applicable, include such information as (1) how often AT&T has shared information with U.S. or foreign government entities; (2) what type of customer information was shared; (3) the number of customers affected; (4) type of government requests; and (5) discussion of efforts by the company to protect customer privacy rights.” In his January 24 Response, Mr. Lewis states that the Proposal “imposes no expectation or request” for the Company to make disclosures that would be contrary to existing laws and regulations.

The AT&T Transparency Report contains the following information regarding government demands for customer information:

National Security Demands

- National Security Letters received in 2013, broken out by:
 - Total received (reported in a range as required by law)
 - Number of customer accounts (reported in a range as required by law)
- Foreign Intelligence Surveillance Act orders received from January 1, 2013 to June 30, 2013 (reflecting the six-month delay required by law), broken out by:
 - Total content and customer accounts (reported separately in ranges as required by law)
 - Total non-content and customer accounts (reported separately in ranges as required by law)

Total U.S. Criminal & Civil Litigation Demands

- Total government demands for information (Federal, State and Local) received in 2013, broken out by:
 - Subpoenas – criminal and civil separately reported
 - Court orders – historic information and real time information separately reported
 - Search warrants – stored content separately reported from all others
- Number of government demands in which there was partial or no data provided by AT&T, broken out by:
 - Rejected/challenged
 - Partial or no information
- Number of court order and search warrant demands for location information, broken out by:
 - Historical information
 - Real-time information
 - Cell tower searches

Emergency Requests

- Number of emergency requests for information, broken out by:
 - 911
 - Exigent

International

- Number of international government demands for information stored in their countries received in 2013, broken out by:
 - Law enforcement
 - URL/IP (website/Internet address) blocking requests

The AT&T Transparency Report provides all of the information about National Security Letters and FISA orders permitted to be disclosed by the Department of Justice's Option One. Equally important, the AT&T Transparency Report compares favorably to the Proposal in all respects. The AT&T Transparency Report provides information about:

- “(1) how often AT&T has shared information with U.S. or foreign government entities” in 2013 – broken down among numerous categories, including separate reporting of aggregate data regarding national security process, as permitted by law;
- “(2) what type of customer information was shared” – for example, subpoenas are typically used “to obtain written business documents, such as calling records”; and court orders are “used in both criminal and civil cases to obtain historical information like billing records or the past location of a wireless device,” as well as in criminal cases to obtain real-time information, such as “wiretap orders, which allow law enforcement to monitor phone calls or text messages while they are taking place, or pen register/‘trap and trace’ orders, which provide information and phone numbers for all calls as they are made or received”;
- “(3) the number of customers affected” in 2013 – for example, between 4,000-4,999 customer accounts were affected by National Security Letters, between 35,000-35,999 customer accounts were affected by FISA orders for content data, and between 0-999 customer accounts were affected by FISA orders for non-content data;
- “(4) type of government requests” received in 2013 – including both civil and criminal subpoenas, court orders, search warrants, emergency requests, NSLs and FISA orders; and
- “(5) discussion of efforts by the company to protect customer privacy rights” – as noted in our December 5, 2013 letter, AT&T has separately discussed its efforts to protect customer privacy rights in the AT&T Privacy Policy,⁴ in the AT&T Code of

⁴ See AT&T Privacy Policy (available at <http://www.att.com/gen/privacy-policy?pid=2506>).

Business Conduct,⁵ and in the Introduction to the AT&T Transparency Report, among other places.

The Proposal also states that AT&T's "reports should be prepared with consideration of existing Transparency (or Law Enforcement Request) Reports published by the major internet companies...." We have reviewed the most recent versions of the transparency reports published by the recipients of the January 27, 2014 Department of Justice Letter (Facebook, Google, LinkedIn, Microsoft, and Yahoo!), and the AT&T Transparency Report is on a par with these companies' implementation of the Department of Justice guidance in their transparency reports:

- Facebook: <http://newsroom.fb.com/Content/Detail.aspx?ReleaseID=797&NewsAreaID=2&ClientID=1>;
- Google: <http://googleblog.blogspot.com/2014/02/shedding-some-light-on-foreign.html>;
- LinkedIn: http://help.linkedin.com/app/answers/detail/a_id/41878;
- Microsoft: http://blogs.technet.com/b/microsoft_on_the_issues/archive/2014/02/03/providing-additional-transparency-on-us-government-requests-for-customer-data.aspx; and
- Yahoo!: <http://yahoo.tumblr.com/post/75496314481/more-transparency-for-u-s-national-security-requests>.

In short, with the publication of the AT&T Transparency Report and its commitment to publish additional Reports on a semi-annual basis, AT&T has substantially implemented the Proposal because the Report compares favorably to the Proposal. Accordingly, the Company believes that the Proposal may be excluded from its 2014 Proxy Materials pursuant to Rule 14a-8(i)(10) – "to avoid the possibility of shareholders having to consider matters which have already been favorably acted upon by the management." Release No. 34-12598 (July 7, 1976).

CONCLUSION

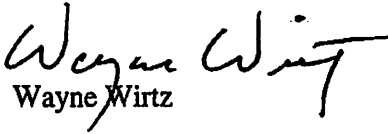
Based upon the foregoing analysis, in addition to the arguments set forth in our December 5, 2013; December 27, 2013; and January 20, 2014, letters, we respectfully request that the Staff concur that it will take no action if the Company excludes the Proposal from its 2014 Proxy Materials.

We would be happy to provide you with any additional information and answer any questions that you may have regarding this subject. Correspondence regarding this letter should be sent to me at ww0118@att.com. If I can be of any further assistance in this matter, please do not hesitate to contact me at (214) 757-3344.

⁵ See AT&T Code of Business Conduct (available at: http://www.att.com/Common/about_us/downloads/att_code_of_business_conduct.pdf).

U.S. Securities and Exchange Commission
February 17, 2014
Page 7

Sincerely,


Wayne Wirtz

Attachment: AT&T Transparency Report

cc: Sanford Lewis, Sarah Nelson, Louise Rice, Tamara Davis, John Silva, Shana Weiss



AT&T

Transparency Report

© 2014 AT&T Intellectual Property. All rights reserved. AT&T and the AT&T logo are trademarks of AT&T Intellectual Property.





Introduction to this report

We take our responsibility to protect your information and privacy very seriously, and we pledge to continue to do so to the fullest extent possible and always in compliance with the law of the country where the relevant service is provided. Like all companies, we must provide information to government and law enforcement agencies to comply 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 provides specific information for all of 2013 regarding the number and types of demands to which we responded, with the exception of certain information that the Department of Justice allows us to report only for the first six months of the year. In the future, we'll issue reports on a semi-annual basis.

Our commitment to you

Interest in this topic has increased in the last year. As you might expect, we may make adjustments to our reporting processes and create ways to track forms of demands in the future. We're committed to providing you with as much transparency and accuracy in this reporting as is possible. This includes:

- Including new information as we are allowed by government policy changes.
- Considering ways to enhance the detail provided in this report as we begin to track these demands consistent with what can be reported publicly.

NATIONAL SECURITY DEMANDS	
National Security Letters (Jan. 1-Dec. 31, 2013) <ul style="list-style-type: none"> Total Received Number of Customer Accounts 	2,000-2,999 4,000-4,999
Foreign Intelligence Surveillance Act (Jan. 1-June 30, 2013) <ul style="list-style-type: none"> Total Content <ul style="list-style-type: none"> Customer Accounts Total Non-Content <ul style="list-style-type: none"> Customer Accounts 	0-999 35,000-35,999 0-999 0-999

TOTAL U.S. CRIMINAL & CIVIL LITIGATION DEMANDS			
Total Demands (Federal, State and Local; Criminal and Civil)			301,816
<ul style="list-style-type: none"> Subpoenas <ul style="list-style-type: none"> Criminal Civil 	223,659 24,684	248,343	
<ul style="list-style-type: none"> Court Orders <ul style="list-style-type: none"> Historic Real-time 	16,478 20,310	36,788	
<ul style="list-style-type: none"> Search Warrants <ul style="list-style-type: none"> Stored Content All Others 	5,690 10,995	16,685	

PARTIAL OR NO DATA PROVIDED (Breakout detail of data included in Total U.S. Criminal & Civil Litigation)		
Total		17,463
<ul style="list-style-type: none"> ▪ Rejected/Challenged ▪ Partial or No Information 	3,756 13,707	

LOCATION DEMANDS (Breakout detail of data included in Total U.S. Criminal & Civil Litigation)		
Total		37,839
<ul style="list-style-type: none"> ▪ Historical ▪ Real-time ▪ Cell Tower Searches 	24,229 12,576 1,034	

EMERGENCY REQUESTS		
Total		94,304
<ul style="list-style-type: none"> ▪ 911 ▪ Exigent 	74,688 19,616	

INTERNATIONAL		
Total Demands		22
<ul style="list-style-type: none"> ▪ Law Enforcement ▪ URL/IP Blocking 	11 11	



Explanatory Notes

NATIONAL SECURITY DEMANDS

Recent guidance by the United States Department of Justice has authorized us to report on the receipt of National Security Letters and court orders issued under the Foreign Intelligence Surveillance Act (FISA). 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 direct communications providers 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 regarding our ability to disclose the requests. On January 27, 2014, the Department of Justice provided new guidance that authorizes us to disclose certain information, in a specified manner, related to the National Security Letters and Foreign Intelligence Surveillance Act Orders we have received. See, <http://www.justice.gov/opa/pr/2014/January/14-ag-081.html>.

Consistent with the guidance of the Department of Justice, 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. Civil actions include lawsuits involving private parties, (a divorce case, for example) and investigations by government regulatory agencies such as the Securities and Exchange Commission, the Federal Trade Commission and the Federal Communications Commission. This total does not include demands reported in our National Security Demands table.

How do we decide if we should respond to a demand?

We determine whether we have received the correct type of demand (such as a subpoena, court order or search warrant) based on federal, state or local laws and what information is 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. Regardless of jurisdiction, we require a court order or search warrant for real-time information, stored content such as text and voice messages, and all location requests by law enforcement.

Subpoenas, Court Orders and Search Warrants are used by law enforcement and attorneys in civil litigation to demand information for use in criminal and civil investigations, trials and other proceedings. If the applicable rules are followed, we're legally required to provide the information.

- **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.
- **Court Orders** are signed by a judge. They are used in both criminal and civil cases 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 information. This can include wiretap orders, which allow law enforcement to monitor phone calls or text messages while they are taking place, or pen register/"trap and trace" orders, which provide information and phone numbers for all calls as they are made or received.
- **Search Warrants** are signed by a judge, and they require law enforcement to show evidence to the court that there is probable cause to believe the information requested by the warrant is evidence of a crime. They are used only in criminal cases, and they are almost always required to obtain real-time location information

CUSTOMERS IMPACTED

We would like to be able to provide information in this report related to the number of customers impacted by criminal and civil demands for their information. However, demands for information in civil or criminal matters involve a wide range of variables – making it very difficult to tally the number of customers whose information was provided in response to those demands. Some law enforcement demands and demands from civil litigants may ask us for records about a particular customer by name and address. However, many demands ask us to

search our records for information related to a particular data point or multiple data points – such as a telephone number, an IP address, a Social Security Number, or date of birth. And data points for multiple customers and accounts often are included in a single demand. Likewise, we have instances where multiple demands focus on one customer.

We also are asked to search for information based on equipment data points. For example, we can be asked to perform cell tower searches that require us to provide all telephone numbers registered on a particular cell tower for a certain period of time, or to confirm whether a specific telephone number registered on a particular cell site at a particular time. The cell tower may be identified by its ID number, its latitude/longitude, or by the street address it serves. The telephone numbers we are required to produce in connection with these searches may belong to our customers and to non-customers as well.

For these reasons we are not able to provide reliable information on the number of customers potentially impacted by these criminal and civil demands for information.

PARTIAL OR NO DATA PROVIDED

In this category we include the number of times we didn't provide information, or provided only partial 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 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.

EMERGENCY REQUESTS

This category includes the number of times we responded to 911-related inquiries and “exigent requests.” These are emergency requests from law enforcement working on kidnappings, missing person cases, attempted suicides and other emergencies.

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

- When responding to 911 inquiries, we automatically 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’re required to comply with requests to block access to websites that are deemed offensive, illegal, unauthorized or otherwise inappropriate in certain countries. These requests might block sites related to displaying child pornography, unregistered and illegal gambling, defamation, illegal sale of medicinal products, trademark and copyright infringement.

We received relatively few international demands because our global business operations support business customers, 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 a 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.

SANFORD J. LEWIS, ATTORNEY

January 24, 2014

Office of Chief Counsel
Division of Corporation Finance
U.S. Securities and Exchange Commission
100 F Street, N.E.
Washington, D.C. 20549

Re: Supplemental Reply Regarding Shareholder Proposal Submitted to AT&T
Requesting Transparency Report on Government Requests for Information

Via electronic mail to shareholderproposals@sec.gov

Ladies and Gentlemen:

The Comptroller of the State of New York, Thomas P. DiNapoli, on behalf of the New York State Common Retirement Fund (the "Fund" or "Proponent") has submitted a shareholder proposal to AT&T Inc. ("AT&T" or the "Company") requesting that the Company issue "transparency reports" on government requests for consumer information (the "Proposal"). On January 20, 2014, Wayne A. Wirtz submitted a supplemental reply (*Company Letter III*) following up on the Company's prior correspondence of December 4, 2013 (*Company Letter I*) and December 27, 2013 (*Company Letter II*).

On January 6, 2014, Proponent submitted a response to Company Letter I and Company Letter II ("Proponent Letter I"). The following is in reply to Company Letter III. A copy of this letter is being emailed concurrently to Mr. Wirtz.

In its latest letter, the Company makes two new assertions: first, that the Proposal "as now interpreted by the Proponent" would cause the Company to violate federal law; and second, that "as interpreted by the Proponent" the Proposal is so vague and indefinite so as to be inherently misleading.

The Proposal does not ask, nor would its implementation cause, the Company to violate federal law. To the contrary, the plain language of the Proposal requests "that the Company publish semi-annual reports, *subject to existing laws and regulation*," (emphasis added), and Proponent Letter I acknowledged that disclosures related to national surveillance might be limited under current law.

Substantial reporting on government information requests, beyond the scope of the Company's proposed report (as described in its press release), including information regarding metadata disclosures to federal, state and local governments, is possible without violating existing law, including the prohibition on national surveillance disclosures. To understand what information the Proponent is seeking, it is important to distinguish between release of classified information, which is unlawful, and the disclosure of information

"regarding" certain classified information that is presented in an aggregated format, which has been lawfully disclosed by Internet companies and, very recently, by Verizon Communications, Inc. ("Verizon"). It is the latter category that the Proposal requests. A review of approaches taken to this issue by various Internet companies demonstrates that such reporting is indeed possible without violating federal law. Contrary to Company Letter III, Internet companies have done substantial reporting regarding their relationship to the national security infrastructure. The Company could implement a similar approach with respect to its report. Indeed, as of January 22, 2014, Verizon, a leading telecom peer of AT&T, issued a transparency report and disclosed a number representing the range of National Security Letters received last year.

The Proposal requests periodic reporting rather than a single report. The Company acknowledges, in Company Letter III, a proposal of the Presidential Review Group that could enable future reporting of information related to national surveillance. Such disclosures could well extend beyond the Foreign Intelligence Surveillance Act ("FISA") letter disclosures released by Verizon. Legislation implementing such a change could be enacted even prior to publication of the proxy. In contrast, AT&T's news release promising a future disclosure report specifically rules out any disclosures by the Company regarding classified information.

For the reasons stated above, the Proposal is not vague and indefinite and, therefore, not misleading, and does not request or require that the Company violate federal law.

1. Proponent Letter I expressly recognized the limitations imposed by the national security laws; Proponent's reply cannot be construed as a request to the Company to violate federal law.

Proponent Letter I expressly recognized in Footnote 30 that Recommendation No. 9 of President Obama's Review Group report stated:

We recommend that legislation should be enacted providing that, even when nondisclosure orders are appropriate, recipients of National Security Letters, section 215 orders, pen register and trap-and-trace orders, section 702 orders, and similar orders issued in programs whose existence is unclassified may publicly disclose on a periodic basis general information about the number of such orders they have received, the number they have complied with, the general categories of information they have produced, and the number of users whose information they have produced in each category, unless the government makes a compelling demonstration that such disclosures would endanger the national security."

The footnote concluded with express recognition of the legal limits on the ability of the Company to reply in the absence of such enactment:

In the absence of such an enactment, some of the summary information requested under the current Proposal might be excluded from reports by the Company to the extent such disclosures are determined by the Company to be prohibited "subject to existing law."

2. The Proposal requests transparency of information that is not subject to restrictions of existing law.

Company Letter III asserts that it would be unlawful for AT&T to disclose information related to national security arrangements. As emphasized in Proponent Letter I, the Proposal contains explicit limitations on disclosure "subject to existing law." Nonetheless, it is clear that publishing some information related to the National Security Agency ("NSA") activities can be done within the confines of existing law.

Under existing law on January 22, 2014, Verizon published a transparency report and included a listing of the range of FISA letters it had received in 2013, after receiving permission from the federal government to publish such a figure. Verizon's announcement of the report noted:

We have obtained permission, however, to report – within a range – the number of National Security Letters we received in 2013. Last week, President Obama announced that telecommunications providers will be permitted to make public more information in the future; we encourage greater transparency and, if permitted, will make those additional disclosures.¹

Verizon's report itself notes receiving between 1,000 and 1,999 National Security Letters in 2013.²

Separate from the ability AT&T has to obtain permission for disclosure from federal authorities, and contrary to the Company's latest assertions, not all metadata sharing is protected by the national surveillance laws. As noted in the background section of Proponent Letter I, metadata sharing has reportedly occurred with agencies other than the NSA, including the Drug Enforcement Administration. Additionally, the telecommunication companies routinely provide wireless metadata as well as call content to other federal, state and local officials.

3. Contrary to Company Letter III, Internet companies DO report information relative to National Security Letters, and national surveillance.

In Company Letter III, AT&T erroneously asserts as part of its Rule 14a-8(i)(3) argument, that none of the Internet companies "disclose information regarding alleged communications intelligence activities of the United States." Accordingly, the Company asserts the Proponent's assertion that the Internet companies' disclosures provide a useful guideline for disclosures in this arena renders the proposal vague and misleading. *Company*

¹ <http://publicpolicy.verizon.com/blog/entry/verizon-releases-first-transparency-report>

² <http://transparency.verizon.com/us-data>

Letter III, page 4.

Quite to the contrary of the Company's assertion, the Internet companies DO report certain information related to national security letters that are responsive to the requests of the Proposal.³ The following examples of Internet company reporting demonstrate that a level of reporting on NSA and/or national surveillance matters is possible under existing law, contrary to the Company's erroneous assertion that it is powerless under existing law to report information related to national surveillance arrangements.

Microsoft notes in its transparency report,⁴ that “We have summarized, per government direction, the aggregate volume of National Security Letters we have received.” It also notes:

We believe this data is valuable and useful to the community that is looking to better understand these issues. However we recognize that this report—focused on law enforcement and excluding national security—only paints part of the picture. We believe the U.S. Constitution guarantees our freedom to share more information with you and are therefore are currently petitioning the federal government for permission to publish more detailed data relating to any legal demands we may have received from the U.S. pursuant to the Foreign Intelligence Surveillance Act (FISA).”

“In June we published aggregate data which showed the combined totals of all requests from US government agencies for the second half of 2012, including if we received them, national security orders. While we believe that had some value in *quantifying the overall volume of requests we received*, it is clear that the continued lack of transparency makes it very difficult for the community—including the global community—to have an informed debate about the balance between investigating crimes, keeping communities safe, and personal privacy.”

In addition, a Microsoft news release from June 14, 2013⁵ notes:

This afternoon, the FBI and DOJ have given us permission to publish some additional data, and we are publishing it straight away. However, we continue to believe that what we are permitted to publish continues to fall short of what is needed to help the community understand and debate these issues.

Here is what the data shows: **For the six months ended December 31, 2012,**

³ Note that the Proposal requests disclosure of both data points regarding government information requests as well as narrative discussion, “of efforts by the Company to protect customer privacy rights.” Supporting Statement, (5).

⁴ <http://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/>

⁵ http://blogs.technet.com/b/microsoft_on_the_issues/archive/2013/06/14/microsoft-s-u-s-law-enforcement-and-national-security-requests-for-last-half-of-2012.aspx

Microsoft received between 6,000 and 7,000 criminal and national security warrants, subpoenas and orders affecting between 31,000 and 32,000 consumer accounts from U.S. governmental entities (including local, state and federal). This only impacts a tiny fraction of Microsoft’s global customer base.

We are permitted to publish data on national security orders received (including, if any, FISA Orders and FISA Directives), but only if aggregated with law enforcement requests from all other U.S. local, state and federal law enforcement agencies; only for the six-month period of July 1, 2012 thru December 31, 2012; only if the totals are presented in bands of 1,000; and all Microsoft consumer services had to be reported together.

We previously published aggregated data for law enforcement requests for the twelve months ended December 31, 2012 in our Law Enforcement Requests Report; but because the national security orders prohibit us from disclosing their existence, we could not include them in that data set.

We have not received any national security orders of the type that Verizon was reported to have received that required Verizon to provide business records about U.S. customers.

We appreciate the effort by U.S. government today to allow us to report more information. We understand they have to weigh carefully the impacts on national security of allowing more disclosures. With more time, we hope they will take further steps. Transparency alone may not be enough to restore public confidence, but it’s a great place to start.

As one can see reading this information from Microsoft, that company was able to publish quite a bit of information about its arrangements with the federal government, including information relating to the national security requests.

As another example, Facebook published its first transparency report (“Global Government Requests Report”) in August 2013, including a “range” of numbers for the United States reflecting the limitations imposed by the federal government on national security related disclosures:

We have reported the numbers for all criminal and national security requests to the maximum extent permitted by law... We will publish updated information for the United States as soon as we obtain legal authorization to do so.

The Yahoo! transparency report in September 2013⁶ also details some of the ways that the company has worked to protect consumers’ privacy the face of government information requests. Also, Google’s Transparency report contains specific information regarding National Security Letters process and its interactions with the federal government.⁷

Company Letter III, therefore, is inaccurate in its assertion that none of the Internet companies disclose information regarding alleged communications intelligence activities of the United States. Further, the fact that the Internet companies cited above and Verizon have done so belies the Company’s position that it is powerless under existing law to make such disclosures, as well as the Company’s assertions of vagueness.

4. As a periodic report, the scope of promised reporting could encompass more.

The proposed amendments to law noted above may expand the Company’s future options of reporting to encompass additional national surveillance information. Legislative action may occur before or after the shareholder meeting. Since the Proposal requests a periodic report, future reports may be able to legally include even more information than the Internet companies currently disclose. But, in contrast, the Company’s news release expressly states its position that any information regarding classified information should come from the federal government, rather than the Company, and further, that its disclosures would be limited to government requests related to “criminal cases” only.⁸ Most importantly the news release stated:

Finally, in our view, **any disclosures regarding classified information should come from the government**, which is in the best position to determine what can be lawfully disclosed and would or would not harm national security. [emphasis added] *AT&T News Release announcing Transparency Report*⁹

This statement effectively forecloses the disclosure of even aggregate information as other companies already are doing.

⁶ <http://yahoo.tumblr.com/tagged/transparency>

⁷ <http://www.google.com/transparencyreport/userdatarequests/>

⁸ The news release states that “To the extent permitted by laws and regulations, AT&T’s transparency report will include:

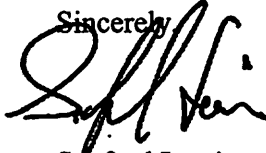
- The total number of law enforcement agency requests received from government authorities in criminal cases;
- Information on the number of subpoenas, court orders and warrants;
- The number of customers affected; and
- Details about the legal demands AT&T receives, as well as information about requests for information in emergencies.”

⁹ <http://www.prnewswire.com/news-releases/att-update-on-government-surveillance-position-236750591.html>

CONCLUSION

For the reasons noted above, the Proposal imposes no expectation or request for the company to violate federal law, nor is the Proposal vague or misleading. The Company has not met its burden of proving that the Proposal is excludable. Therefore, we request that the Staff inform the Company that the SEC proxy rules require denial of the Company’s no-action request.

Sincerely,

A handwritten signature in black ink, appearing to read "Sanford Lewis", written over the word "Sincerely,".

Sanford Lewis
Attorney at Law

cc: Comptroller Thomas P. DiNapoli
Wayne A. Wirtz, AT&T



Wayne A. Wirtz
Associate General Counsel
Legal Department
208 S. Akard, Room 3024
Dallas, Texas 75202
(214) 757-3344
ww0118@att.com

1934 Act/Rule 14a-8

By email: shareholderproposals@sec.gov

January 20, 2014

U.S. Securities and Exchange Commission
Division of Corporation Finance
Office of Chief Counsel
100 F St., NE
Washington, DC 20549

Re: AT&T Inc. – Second Supplemental Request to Exclude Shareholder Proposal of the New York State Common Retirement Fund et al.

Ladies and Gentlemen:

On December 5, 2013, AT&T Inc., a Delaware corporation (“AT&T” or the “Company”), submitted a letter stating its intent to exclude from its proxy statement and form of proxy for its 2014 Annual Meeting of Shareholders (collectively, the “2014 Proxy Materials”) a shareholder proposal (the “Proposal”) and statement in support thereof (the “Supporting Statement”) submitted by the New York State Common Retirement Fund and co-filers Sarah Nelson, Louise Rice, Tamara Davis, John Silva and Shana Weiss (collectively, the “Proponents”). The Proposal requests that the Company “publish semi-annual reports, subject to existing laws and regulations, providing metrics and discussion regarding requests for customer information by U.S. and foreign governments, at reasonable cost and omitting proprietary information.”

On December 20, 2013, AT&T issued a press release announcing its intent to publish a Transparency Report disclosing law enforcement requests for customer information that AT&T received in 2013 in the United States and the other countries in which it does business (the “AT&T Transparency Report”). In light of this announcement, on December 27, 2013, AT&T supplemented its December 5, 2013 letter with a letter to the Staff adding a separate argument to exclude the Proposal pursuant to Exchange Act Rule 14a-8(i)(10) – substantial implementation.

On January 6, 2014, Sanford J. Lewis, counsel for the Proponents, submitted a response to the Company’s December 5 and December 27 letters (the “Response”). The Response asserts that the AT&T Transparency Report “would reflect only a small fragment of the disclosure required by the Proposal” and would not substantially implement the Proposal because

“disclosures related to meta-data sharing with the NSA and any similar programs...would be excluded.” And yet, the Response also states that, “**The current Proposal is essentially a request to AT&T to engage in reporting on par with the transparency reports of the internet companies**” (emphasis in original). None of the Transparency Reports issued by the major Internet companies include specific information about meta-data sharing with the NSA and any similar programs.

In light of the new information contained in the Response, the Company believes that the Proposal can be excluded on two new grounds: Rule 14a-8(i)(2) and Rule 14a-8(i)(3).

ARGUMENT

The Proposal May Be Excluded Pursuant to Exchange Act Rule 14a-8(i)(2) Because the Proposal, as Now Interpreted by Proponent, Would Cause the Company to Violate Federal Law.

Rule 14a-8(i)(2) permits a company to exclude a shareholder proposal if implementation of the Proposal would cause the company to violate any state, federal or foreign law to which it is subject.

The Proposal requests that the Company “publish semi-annual reports, subject to existing laws and regulations, providing metrics and discussion regarding request for customer information by U.S. and foreign governments, at reasonable cost and omitting proprietary information.” The Proposal’s Supporting Statement states that, “[t]he reports should be prepared with consideration of existing Transparency (or Law Enforcement Request) Reports published by the major internet companies, and where applicable, include such information as (1) how often AT&T has shared information with U.S. or foreign government entities; (2) what type of customer information was shared; (3) the number of customers affected; (4) type of government requests; and (5) discussion of efforts by the company to protect customer privacy rights.”

On December 20, 2013, AT&T issued a press release announcing its intent to publish the AT&T Transparency Report. AT&T expects to publish its first AT&T Transparency Report in early 2014 and to update it semi-annually. The AT&T Transparency Report will include, to the extent permitted by laws and regulations:

- The total number of law enforcement agency requests received from government authorities in criminal cases;
- Information on the number of subpoenas, court orders and warrants;
- The number of customers affected; and
- Details about the legal demands AT&T receives, as well as information about requests for information in emergencies.

In light of this decision, in its December 27, 2013 letter, the Company argued that the AT&T Transparency Report substantially implements the Proposal because it will contain information that compares favorably with the information requested by the Proposal and it

satisfies the Proposal's essential objective. The AT&T Transparency Report will be published semi-annually, as requested by the Proposal; it will disclose the total number of law enforcement agency requests received from government authorities in criminal cases, which satisfies "(1) how often AT&T has shared information with U.S. or foreign government entities"; it will disclose the number of customers affected, which satisfies "(3) the number of customers affected"; and it will disclose the number of subpoenas, court orders and warrants, including details about the legal demands AT&T receives, as well as information about requests for information in emergencies, which satisfy "(4) type of government requests". AT&T's Privacy Policy¹ and Code of Business Conduct² already discuss the Company's efforts to protect customer privacy rights, which satisfy "(5) discussion of efforts by the company to protect customer privacy rights."

The Response now states that the AT&T Transparency Report would reflect "only a fragment of the Proposal's request" because the report "would not address the 'millions' of customer call records (metadata) reportedly shared with the government" (p. 2) and "disclosures related to meta-data sharing with the NSA and any similar programs...would be excluded" (p. 26). As the Response interprets the Proposal, it requests AT&T to prepare a report that includes information regarding alleged communications intelligence activities of the United States. In the opinion of our counsel, Sidley Austin LLP, a copy of which is attached to this submission, to the extent such information exists, implementation of the Proposal, as interpreted in the Response, would cause the Company to violate a series of federal laws designed to protect the intelligence gathering activities of the United States, and therefore can be excluded pursuant to Rule 14a-8(i)(2).

The Proposal May Be Excluded Pursuant to Exchange Act Rule 14a-8(i)(3) Because the Proposal, as Now Interpreted by Proponent, Is Impermissibly Vague and Indefinite so as to be Inherently Misleading.

Rule 14a-8(i)(3) provides that a company may exclude a shareholder proposal from its proxy materials if the proposal or supporting statement is contrary to any of the Commission's proxy rules, including Rule 14a-9, which prohibits materially false or misleading statements in proxy solicitation materials. The Staff consistently has taken the position that vague and indefinite shareholder proposals are inherently misleading and therefore excludable under Rule 14a-8(i)(3) because "neither the stockholders voting on the proposal, nor the company in implementing the proposal (if adopted), would be able to determine with any reasonable certainty exactly what actions or measures the proposal requires." Staff Legal Bulletin No. 14B (Sept. 15, 2004). The Staff has further explained that a shareholder proposal can be sufficiently misleading and therefore excludable under Rule 14a-8(i)(3) when the company and its shareholders might interpret the proposal differently such that "any action ultimately taken by the [c]ompany upon implementation [of the proposal] could be significantly different from the

¹ See AT&T Privacy Policy (available at <http://www.att.com/gen/privacy-policy?pid=2506>).

² See AT&T Code of Business Conduct (available at: http://www.att.com/Common/about_us/downloads/att_code_of_business_conduct.pdf).

actions envisioned by the shareholders voting on the proposal.” *Fuqua Industries, Inc.* (Mar. 12, 1991).

The Response now states that the AT&T Transparency Report would reflect “only a fragment of the Proposal’s request” because the report “would not address the ‘millions’ of customer call records (metadata) reportedly shared with the government” (p. 2) and “disclosures related to meta-data sharing with the NSA and any similar programs...would be excluded” (p. 26). And yet, the Proposal’s Supporting Statement states that AT&T’s reports “should be prepared with consideration of existing Transparency (or Law Enforcement Request) Reports published by the major internet companies.” And indeed, the Response confirms this, stating that, **“The current Proposal is essentially a request to AT&T to engage in reporting on par with the transparency reports of the internet companies”** (p.8) (emphasis in original). However, none of the Transparency or Law Enforcement Request Reports issued by Google, Microsoft, Twitter, LinkedIn, Facebook and Yahoo! disclose information regarding alleged communications intelligence activities of the United States – for the stated reason that so doing is not permitted under law.³

How is AT&T’s reporting to be “on par” with the transparency reports issued by the major Internet companies, and yet, at the same time, according to the Response, any such report would reflect “only a fragment of the Proposal’s request” because “disclosures related to meta-data sharing with the NSA and any similar programs...would be excluded”? In light of the Response’s interpretation of the Proposal, we are now of the view that the Proposal is vague and misleading and is therefore excludable under Rule 14a-8(i)(3) because “neither the stockholders voting on the proposal, nor the company in implementing the proposal (if adopted), would be able to determine with any reasonable certainty exactly what actions or measures the proposal requires.” Staff Legal Bulletin No. 14B (Sept. 15, 2004).

CONCLUSION

Based upon the foregoing analysis, in addition to the arguments set forth in our December 5, 2013 and December 27, 2013 letters, we respectfully request that the Staff concur that it will take no action if the Company excludes the Proposal from its 2014 Proxy Materials.

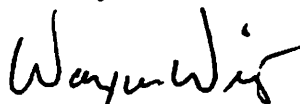
We would be happy to provide you with any additional information and answer any questions that you may have regarding this subject. Correspondence regarding this letter should

³ See, e.g., Microsoft (“Unfortunately, we are not currently permitted to report detailed information about the type and volume of any national security orders (e.g. FISA Orders and FISA Directives) that we may receive so any national security orders we may receive are not included in this report. We have summarized, per government direction, the aggregate volume of National Security Letters we have received.”) (emphasis in original), available at <https://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/>; and Facebook (“We have reported the numbers for all criminal and national security requests to the maximum extent permitted by law. We continue to push the United States government to allow more transparency regarding these requests, including specific numbers and types of national security-related requests. We will publish updated information for the United States as soon as we obtain legal authorization to do so.”), available at https://www.facebook.com/about/government_requests.

U.S. Securities and Exchange Commission
January 20, 2014
Page 5

be sent to me at ww0118@att.com. If I can be of any further assistance in this matter, please do not hesitate to contact me at (214) 757-3344.

Sincerely,


Wayne Wirtz

Attached: Opinion of Sidley Austin LLP

cc: Sanford Lewis, Sarah Nelson, Louise Rice, Tamara Davis, John Silva, Shana Weiss



SIDLEY AUSTIN LLP
1501 K STREET, N.W.
WASHINGTON, D.C. 20005
(202) 738 8000
(202) 738 8711 FAX

BEIJING
BOSTON
BRUSSELS
CHICAGO
DALLAS
FRANKFURT
GENEVA

HONG KONG
HOUSTON
LONDON
LOS ANGELES
NEW YORK
PALO ALTO
SAN FRANCISCO

SHANGHAI
SINGAPORE
SYDNEY
TOKYO
WASHINGTON, D.C.

FOUNDED 1866

January 20, 2014

Board of Directors
AT&T Inc.
c/o Wayne Watts
General Counsel
208 South Akard Street
Dallas, TX 75202

Re: Shareholder Proposal

Ladies and Gentlemen:

You have requested our legal opinion whether it would violate federal law for AT&T Inc. ("AT&T" or the "Company") to implement a shareholder proposal (the "Proposal") that has been submitted by the New York State Common Retirement Fund and co-filers Sarah Nelson, Louise Rice, Tamara Davis, John Silva, and Shana Weiss (collectively, the "Proponents") for inclusion in the Company's proxy statement for the 2014 Annual Meeting of Shareholders.

The Proposal. The Proposal calls for the Company to "publish semi-annual reports, subject to existing laws and regulation, providing metrics and discussion regarding requests for customer information by U.S. and foreign governments, at reasonable cost, and omitting proprietary information."¹ These semi-annual reports "should . . . include" disclosures of (1) "how often" AT&T has shared information with U.S. or foreign government entities; (2) "what type of customer information was shared;" (3) the "number of customers affected;" (4) the "type of government request;" and (5) "discussion of efforts by the [C]ompany to protect the privacy of such customer data." Even though the Proposal asks for metrics on any "requests . . . by U.S. and foreign governments," the Proposal's Supporting Statement provides that AT&T "may, at its discretion, omit information on routine requests provided under individualized warrants."

According to the Proponents, some "major Internet companies" have published "'Transparency Reports,' disclosing information on government requests." These "transparency" reports generally provide highly aggregated data on government requests for

¹ Available at http://www.osc.state.ny.us/reports/pension/CRF_ATT_DataPrivacy2014_Resolution.pdf

data.² The reports do not, however, include information on what type of customer information was shared or the type of government request – for example, there is no indication whether these companies have disclosed information to the National Security Agency (“NSA”) or Federal Bureau of Investigation (“FBI”) pursuant to the Foreign Intelligence Surveillance Act (“FISA”) or other laws requiring such disclosures.

No-Action Request. On December 5, 2013, AT&T submitted a letter with the Staff of the Securities and Exchange Commission (“SEC”) stating its intent to exclude the Proposal from its proxy statement and form of proxy for its 2014 Annual Meeting of Shareholders (“2014 Proxy Materials”).³ AT&T provided several grounds to justify the exclusion, and asked that the SEC Staff concur that it will take no action if AT&T excludes the Proposal from its 2014 Proxy Materials.

On December 20, 2013, AT&T issued a press release announcing its intent to publish a Transparency Report disclosing law enforcement requests for customer information that AT&T received in 2013 in the United States and the other countries in which it does business (the “AT&T Transparency Report”).⁴ As stated in that press release, AT&T expects to publish its first AT&T Transparency Report in early 2014 and to update it semi-annually. The AT&T Transparency Report will include, to the extent permitted by laws and regulations:

- The total number of law enforcement agency requests received from government authorities in criminal cases;
- Information on the number of subpoenas, court orders and warrants;
- The number of customers affected; and
- Details about the legal demands AT&T receives, as well as information about requests for information in emergencies.

On December 27, 2013, AT&T filed a supplemental request to exclude the proposal, stating that, in light of the forthcoming AT&T Transparency Report, the Proposal has been substantially

² The reports provided by Microsoft, for example, disclose the total number of requests Microsoft received from over 50 countries, including the United States. The reports disclose the number of accounts/users specified in the requests and the percentage of requests that result in disclosure of “content” or disclosure of “non-content data.” <https://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/>

³ Available at <http://www.sec.gov/divisions/corpfin/cf-noaction/14a-8/2013/nystatecommon120513-14a8-incoming.pdf>

⁴ Available at <http://www.prnewswire.com/news-releases/att-update-on-government-surveillance-position-236750591.html>

implemented.⁵ AT&T claimed that, of the five categories of information identified in the Proposal's Supporting Statement, the AT&T Transparency Report addresses all categories, except "what type of customer information was shared." As noted, the transparency reports issued by Internet companies, which the Proposal states should be considered by AT&T, also do not include this type of disclosure.

On January 6, 2014, counsel for the Proponents submitted a lengthy response to the SEC.⁶ After again emphasizing that the Proposal's concern was with allegations that AT&T had provided call records to the NSA or other government agencies, the Proponents' Response argued that the AT&T Transparency Report would not substantially implement the Proposal. The Proponents' Response claimed that AT&T's Transparency Report "would reflect only a small fragment of the disclosure required by the Proposal." *Id.* at 26. In particular, the Proponents' Response argued that the AT&T Transparency Report would not substantially implement the Proposal because "disclosures related to meta-data sharing with the NSA and any similar programs . . . would be excluded." *Id.*

As the Proponents' Response makes especially clear, therefore, the Proponents interpret their own Proposal as asking for reports that include information about NSA activities (and those of other similar agencies), notwithstanding the references to using the Internet companies' Transparency Reports as examples to follow and notwithstanding the qualification that the report would be "subject to existing laws and regulation."

L. Analysis and Discussion

A. Relevant Legal Framework. *Federal Criminal Prohibition On Disclosure Of Classified Information Concerning The Communication Intelligence Activities Of The United States.* It is a felony under federal law to knowingly and willfully divulge to an unauthorized person classified information regarding the communications intelligence activities of the United States. In particular, 18 U.S.C. § 798(a) provides:

Whoever knowingly and willfully communicates, furnishes, transmits, or otherwise makes available to an unauthorized person, or publishes, or uses in any manner prejudicial to the safety or interest of the United States, or for the benefit of any foreign government to the detriment of the United States any classified information –

⁵ Letter of W. Wirtz, counsel for AT&T, to Office of Chief Counsel, Division of Corporation Finance, SEC, Dec. 27, 2013.

⁶ Letter of S. Lewis, counsel for Proponents, to Office of Chief Counsel, Division of Corporation Finance, SEC, Jan. 6, 2014 ("Proponents' Response").

* * * *

- (2) concerning the design, construction, use, maintenance, or repair of any device, apparatus, or appliance used or prepared or planned for use by the United States or any foreign government for cryptographic or communication intelligence purposes; or
- (3) concerning the communication intelligence activities of the United States or any foreign government . . .

* * * *

Shall be fined under this title or imprisoned not more than ten years, or both.

*Id.*⁷

Disclosure of classified information, including the number and scope of requests a company may have received pursuant to FISA, to any “unauthorized person,” including such company’s shareholders, would violate federal law and thereby subject the company to potential criminal liability under this section.⁸

Restrictions on disclosure under FISA and the SCA. In addition to the general prohibition against disclosure of classified information, FISA prohibits disclosure of certain orders of FISA courts and of information that has been disclosed pursuant to such orders. In particular, pursuant to 50 U.S.C. § 1861, the Federal Bureau of Investigation is authorized to

⁷ As defined by this statute, the term “classified information” means “information which, at the time of a violation of this section, is for reasons of national security, specifically designated by a United States Government Agency for limited or restricted dissemination or distribution. . . .” 18 U.S.C. § 798(b). The term “unauthorized person” means “any person, who, or agency which, is not authorized to receive information of the categories set forth in subsection (a) of this section, by the President, or by the head of a department or agency of the United States Government to engage in communication intelligence activities for the United States.” *Id.*

⁸ See also Section 6 of the National Security Agency Act, Pub. L. No. 86-36, § 6, 73 Stat. 63, 64, codified at 50 U.S.C. § 402 note (“nothing in this Act or any other law . . . shall be construed to require the disclosure of the organization or any function of the National Security Agency, or of any information with respect to the activities thereof”); *Linder v. National Security Agency*, 94 F.3d 693, 698 (D.C. Cir. 1996)(“[t]he protection afforded by section 6 is, by its very terms, absolute”); *Founding Church of Scientology v. National Security Agency*, 610 F.2d 824, 828 (D.C. Cir. 1979); *Hayden v. National Security Agency*, 608 F.2d 1381, 1390 (D.C. Cir. 1979).

obtain customer information from telecommunications carriers upon application to a court for a FISA order but without a conventional warrant. When such business records are produced, the carrier is prohibited from disclosing “to any other person that the Federal Bureau of Investigation has sought or obtained tangible things pursuant to an order under this section,” subject to certain exceptions not applicable here. *Id.* § 1861(d).

FISA contains an additional section, 50 U.S.C. § 1802(a)(4), which provides that where electronic surveillance occurs pursuant to FISA without any type of court order (as it may under certain circumstances), a carrier may be directed by the Attorney General to protect the secrecy of such surveillance and adhere to prescribed security procedures to ensure that is done, and the carrier must comply with the directive.

Additionally, under provisions of the Stored Communications Act, the Director of the FBI is authorized to demand and obtain from a wire or electronic communication service provider transactional, billing, or calling records without any form of court order, and in many circumstances, the carrier is categorically barred from disclosing receipt or fulfillment of such a request, again subject to exceptions not applicable here. *See* 18 U.S.C. § 2709(c).

As interpreted by the Proponents, the Proposal seeks information in each of the above categories, to the extent such information exists.

B. Assessment of Legality of Proposal.

As the Proponents interpret their Proposal, AT&T would violate one or more of the federal laws cited above (the “Referenced Federal Statutes”) if it were to implement the Proposal as interpreted by the Proponents. Although AT&T has asserted that the AT&T Transparency Report would substantially implement the proposal, the Proponents have vigorously disputed this claim. In particular, they assert that the Proposal should be interpreted as requiring, among other information, “disclosures related to meta-data sharing with the NSA and any similar programs.” Proponents’ Response at 26. As further explained below, the Referenced Federal Statutes prohibit precisely these types of disclosures.

Like every other entity, AT&T is barred by the Referenced Federal Statutes from disclosing classified information. As the United States has explained in opposing the requests by some Internet companies to disclose additional details regarding FISA requests they may have received, classified information encompasses more than the contents of any requests (*i.e.*, the identity of the surveillance target) that a communications provider might have received pursuant

to FISA. Rather, classified information also includes “sources and methods of surveillance.”⁹ The United States has thus determined that disclosure of information such as the names of providers responding to FISA requests, the number of FISA requests received by each such provider, and the specific information collected “would provide adversaries significant information about the Government’s collection capabilities with respect to particular providers” – and thereby provide adversaries a guide to avoiding surveillance.¹⁰ Accordingly, the United States would view disclosures of matters such as “how often” AT&T might (or might not) have received requests for information pursuant to FISA and the “type . . . of information shared” in response to any such FISA requests as unlawful disclosures of classified information.

It is well-established that the government’s decision to classify information is subject to “utmost deference.” *Department of the Navy v. Egan*, 484 U.S. 518, 529-30 (1988); *see id.* at 529 (“For ‘reasons . . . too obvious to call for enlarged discussion,’ the protection of classified information must be committed to the broad discretion of the agency responsible, and this must include broad discretion to determine who may have access to it.”) (*quoting CIA v. Sims*, 471 U.S. 159, 170 (1985)). This deference is especially strong in areas of national defense and foreign policy. *See, e.g., Larson v. Dep’t of State*, 565 F.3d 857, 864 (D.C. Cir. 2009) (courts “accord substantial weight to an agency’s affidavit concerning the details of the classified status of [a] disputed record because the Executive departments responsible for national defense and foreign policy matters have unique insights into what adverse [e]ffects might occur as a result of a particular classified record”); *Krikorian v. Dep’t of State*, 984 F.2d 461, 464-65 (D.C. Cir. 1993) (courts “lack the expertise” to “second-guess [] agency opinions” in the “typical national security . . . case” seeking disclosure of classified material).

On January 17, 2014, President Obama gave a speech announcing his intention to pursue various reforms of the nation’s signals intelligence activities, in which he stated his intention to take actions that would “enable communications providers to make public more information than ever before about the orders that they have received to provide data to the government.”¹¹ The President offered no details as to when, how, or to what extent the government would take such actions, which documents, if any, would be declassified, or whether any such reforms would require new legislation given that certain of the disclosure limitations contained in the

⁹ Resp. of the United States to Motions for Declaratory Judgment By Google Inc. *et al.*, at 4, *In re Amended Motion for Decl. Judgment*, Docket Nos. 13-03, *et al.* (Foreign Intell. Surv. Court, filed Sept. 30, 2013) (“DOJ Metrics Response”).

¹⁰ *Id.* at 3-7, 9.

¹¹ *See* “Transcript of President Obama’s Jan. 17 Speech on NSA Reforms,” Washington Post, available at http://www.washingtonpost.com/politics/full-text-of-president-obamas-jan-17-speech-on-nsa-reforms/2014/01/17/fa33590a-7f8c-11e3-9556-4a4bf7bcbdd84_print.html.

Referenced Federal Statutes are statutory prohibitions that do not turn on the classification of the information. Regardless of what reforms the government may adopt in the future, however, AT&T remains subject to the Referenced Federal Statutes today to the extent described in this letter.

As Interpreted By The Proponents, Implementation of the Proposal Would Require AT&T To Make Unlawful Disclosures. AT&T would face liability under one or more of the Referenced Federal Statutes if AT&T were to issue the disclosures that the Proponents claim are called for in the Proposal.

Like the declaratory rulings sought by some Internet companies but opposed by the government, the Proponents' interpretation of the Proposal is premised on the view that the disclosure of "metrics" – *i.e.*, the precise number of the various "type of government requests" that AT&T may (or may not) have received – cannot reveal classified information. Under this view, disclosures regarding the number and type of requests to which a particular provider responds are lawful so long as the particular surveillance targets are not disclosed.

But as the Department of Justice has explained, that

implausible reading ignores the forest for the trees. It would permit damaging disclosures that would reveal sources and methods of surveillance potentially nationwide. The secrecy provisions in the [FISA] orders flow from statutory requirements that, according to their plain language, protect such sources and methods, not just particular collection efforts.¹²

Because "revealing FISA data on a company-by-company basis would cause serious harm to national security, such data has been classified."¹³

In short, while that the Proponents have asserted that the Proposal should be interpreted to require "disclosures related to meta-data sharing with the NSA and any similar programs," the federal government's position is that such information is classified. Given that the President has

¹² DOJ Metrics Response at 4. *See also id.* at 3 (if providers revealed "the nature and scope of any FISA surveillance of their communications platforms," such disclosures "would be invaluable to our adversaries, who could thereby derive a clear picture of where the Government's surveillance efforts are directed and how its surveillance activities change over time, including when the Government initiates or expands surveillance efforts involving providers or services that adversaries previously considered 'safe.'").

¹³ *Id.* at 4; *see also id.* at 7-11 (detailing potential harm from company specific disclosures on number and scope of FISA requests).

authority to determine whether information is appropriately classified and Proponents do not, AT&T's compliance with the Proposal as interpreted by the Proponents would place AT&T at substantial risk for criminal and other sanctions.

The Proposal points to the "transparency reports" that some Internet companies have voluntarily published and that contain certain, highly aggregated disclosures of government requests for information, the implication being that these disclosures necessarily mean that AT&T also could lawfully provide the reports described in the Proposal.

The "transparency" reports that the Internet companies have generally provided to date are different than the reports contemplated by the Proponents. The Internet companies' disclosures contain highly aggregated data of requests from a particular country.¹⁴ But the Proposal as interpreted by the Proponents would require AT&T to make additional disclosures, such as the "type of government requests" it may have received from the NSA, and the "type of customer information" that may have been shared with NSA (or other similar agencies), to the extent such information exists. For the reasons stated above, the United States would consider such information to be classified.

Irrelevance of Authorized Compliance with Law. The legality of the Proposal is not affected by the fact that it states that AT&T's report should be issued "subject to existing laws and regulations." Proponents' Response clearly indicates that it requests disclosure of information regarding classified NSA and FISA information. AT&T could not implement the Proposal and issue the report that Proponents' Response requests without analyzing the cooperation that it has or has not provided these agencies and without at least implicitly providing information that would confirm or deny whether the allegations about AT&T's dealings with national security agencies are true – all of which the United States considers classified information.

II. Opinion.

In rendering our opinion, we have considered the applicable provisions of the United States Code, relevant judicial interpretations, and such other legal authorities as we have

¹⁴ The government has stated that it has "agreed that companies may report the aggregate number of National Security Letters (NSLs) they receive, in numeric ranges and on a periodic basis." DOJ Metrics Response at 1. The government has also agreed to permit "companies to make a wider set of disclosures by opting to report, in certain bands, the aggregate number of criminal and national security related orders they receive from federal, state, and local government entities combined, and the number of user accounts affected by such orders." *Id.* at 2. However, the Proposal as interpreted by the Proponents is not limited to this type of information.



Board of Directors

January 20, 2014

Page 9

considered relevant. It should be noted that such statutes, interpretations, and other authorities are subject to change. Any such changes may be retroactive and could have an effect on the conclusions stated herein.¹⁵

Based on the foregoing facts and analysis regarding the Proposal as recited herein, and subject to the qualifications, assumptions and discussions contained herein, we are of the opinion that the AT&T would violate one or more of the Referenced Federal Statutes if it were to implement the Proposal as interpreted by the Proponents.¹⁶

Sincerely,

A handwritten signature in cursive script that reads "Sidley Austin LLP".

Sidley Austin LLP

DLL

¹⁵ We have assumed the genuineness of all signatures, the proper filing of all documents which purport to be filed with federal agencies, the legal capacity of all natural persons to sign such documents, the authenticity of all documents submitted to us as originals and the conformity with the original documents of all documents submitted to us by electronic transmission.

¹⁶ Our analysis is limited to the facts and assumptions as they are presented herein and is subject to the qualification that there are no additional facts that would materially affect the validity of the assumptions and conclusions set forth herein or upon which this opinion is based. Our conclusions are based on the law specifically referenced here as of the date hereof, we express no opinion as to the laws, rules or regulations not specifically referenced, and we assume no obligation to advise you of changes in the law of fact (or the effect thereof on the Opinion expressed or the statements made herein) that hereafter may come to our attention. Our opinions are limited to the specific opinions expressed in this "Opinion" section. The foregoing assessment is not intended to be a guarantee as to what a particular court would actually hold, but an assessment of a reviewing court's action if the issues were properly presented to it and the court followed what we believe to be the applicable legal principles. This opinion may not be relied upon in whole or in part by any other person or entity other than its addressee without our specific prior written consent. We understand that you intend to attach a copy of this opinion to an additional letter relating to the Proposal to the SEC under the procedures set forth in 17 C.F.R. § 240.14a-8, and we hereby consent to the use of this opinion for that purpose.

SANFORD J. LEWIS, ATTORNEY

January 6, 2014

Office of Chief Counsel
Division of Corporation Finance
U.S. Securities and Exchange Commission
100 F Street, N.E.
Washington, D.C. 20549

Re: Shareholder Proposal Submitted to AT&T Requesting Transparency Report
on Government Requests for Information

Via electronic mail to shareholderproposals@sec.gov

Ladies and Gentlemen:

The Comptroller of the State of New York, Thomas P. DiNapoli, on behalf of the New York State Common Retirement Fund (the "Fund" or "Proponent") has submitted a shareholder proposal to AT&T Inc. ("AT&T" or the "Company") requesting that the Company issue transparency reports on government requests for consumer information (the "Proposal").¹ A letter dated December 4, 2013 (*Company Letter I*) sent to the Securities and Exchange Commission ("SEC" or the "Staff") by Wayne A. Wirtz, Associate General Counsel for the Company contends that the Proposal may be excluded from the Company's 2014 proxy statement under Rule 14a-8(i)(7), asserting that the issues of privacy and transparency relating to government information requests are excludable matters of ordinary business. In addition, Mr. Wirtz submitted a second, supplemental letter to the SEC on December 27, 2013, asserting that the Proposal is substantially implemented and excludable pursuant to Rule 14a-8(i)(10). (*Company Letter II*)

I have been asked by the Proponent to review the Company letters and to respond on his behalf. Based upon the relevant rules, it is my opinion that the Proposal must be included in the Company's 2014 proxy materials. It is not excludable by virtue of Rule 14a-8(i)(7) or Rule 14a-8(i)(10). A copy of this letter is being emailed concurrently to Mr. Wirtz.

The Proposal (included in its entirety in *Exhibit A*) requests that the Company "publish semi-annual reports, subject to existing laws and regulation, providing metrics and discussion regarding requests for customer information by U.S. and foreign governments, at reasonable cost and omitting proprietary information."

¹ The Proposal was also co-filed by Sarah Nelson, Louise Rice (represented by Trillium Asset Management, LLC), Tamara Davis, John Silva and Shana Weiss.

The supporting statement further clarifies that in preparing these reports, “the Company may, at its discretion, omit information on routine requests provided under individualized warrants. The reports should be prepared with consideration of existing Transparency (or Law Enforcement Request) Reports published by the major internet companies, and where applicable, include such information as (1) how often AT&T has shared information with U.S. or foreign government entities; (2) what type of customer information was shared; (3) the number of customers affected; (4) type of government requests; and (5) discussion of efforts by the company to protect customer privacy rights.”

The Company asserts that the Proposal is excludable pursuant to Rule 14a-8(i)(7) as relating to the ordinary business of the Company. However, the Proposal has arisen as the Company finds itself embroiled in a high profile controversy alleging telecom company cooperation in conveying the private calling records of millions of American and foreign citizens to various federal, state and local government entities. This has elevated the issue to front page news status, and has led to major engagement by President Obama and Congress. Therefore the Proposal addresses a significant policy issue that transcends ordinary business and is not excludable.

Further, the issue has already had significant impact on the Company's business relationships and prospects. Customer expectations of trust and privacy have been undermined by recent developments; the nexus of this issue to the Company is clear. The Proposal does not constrain the Company's approach to litigation, is not overly broad, and does not micromanage. Thus, the Proposal is not excludable under Rule 14a-8(i)(7).

The Company also asserts that the Proposal is excludable pursuant to Rule 14a-8(i)(10), as substantially implemented, based on a news release issued by the Company claiming that it will, in the future, issue transparency reports containing some of the elements of the requested reports. Under SEC Rule 14a-8(i)(10) and related Staff precedents, a mere *promise* to fulfill a shareholder proposal's requests in the future cannot constitute substantial implementation. In the absence of a specific report to review, shareholders could find that a company's promise to implement a proposal is later broken, leaving those shareholders without recourse.

In addition, if a report were issued based on the Company's specifications in its press release, addressing “criminal cases” only, it would not attain substantial implementation. Such report would not address the “millions” of customer call records (metadata) reportedly shared with government. Similarly, many requests by foreign governments of political or religious dissidents' phone calls, emails or calling records would not lie within the scope of the Company's intended report. One cannot predict the full range of other information that might be omitted by limiting the report to “criminal cases.” However, the proposed report would clearly reflect only a fragment of the Proposal's request, and fail to address its essential objectives of transparency and rebuilding of trust. Therefore, the Proposal is not excludable pursuant to Rule 14a-8(i)(10).

BACKGROUND

AT&T and other telecom and internet companies are at the center of a firestorm of public concern and debate regarding the circumstances and conditions under which private customer information is shared with government entities. This issue has garnered significant attention of President Obama, Congress and the media, and poses a significant threat to business opportunities for the Company. Elements of the controversy include:

- National Security Agency (“NSA”) acquisition of customer data, including metadata (calling records) as well as content of customer communications, revealed to the public as early as 2005;
- Drug Enforcement Administration (“DEA”) access to similar data;
- The Central Intelligence Agency was reported to contract with telecoms for call records.²
- Revelations regarding extent to which AT&T and other telecommunication companies routinely provide metadata and call content to other federal, state and local officials.

National Security Agency Controversy

In December 2005, *The New York Times* and other media organizations reported that AT&T had an agreement with the federal government, **dating back to 2001**, to systematically gather information flowing on the internet through the Company's network.³ These reports described in particular the construction and operation of an NSA “secret spying room” in AT&T's San Francisco facility, the Study Group 3 Secure Room (SG-3 room), also known as Room 641A.⁴ As a major population hub and international port, the city of San Francisco supports massive volumes of electronic communications on fiber optic trunks that carry Internet backbone traffic through the city and throughout the U.S. According to the reports, the NSA created a complete copy of *all* Internet traffic received by AT&T by using a “splitter” at this key location. The communications tracked included email, web-browsing requests, playback of telephone calls routed on the Internet, and other electronic communications.

Following those reports, more than 40 lawsuits were filed against communications carriers, including AT&T, collectively seeking “hundreds of billions of dollars in damages,” according to the Harvard Law Review. The lawsuits alleged that AT&T's assistance with the government's illegal wiretapping and data-mining program was itself illegal, and constituted

² http://www.nytimes.com/2013/11/07/us/cia-is-said-to-pay-att-for-call-data.html?_r=0

³ The media reports, later substantially verified, were based on disclosures by a retired former AT&T technician.

⁴ Electronic Frontier Foundation, “AT&T's Role in Dragnet Surveillance of Millions of its Customers”
https://www EFF.org/files/filenode/att/presskit/ATT_onepager.pdf

an invasion of privacy.⁵ AT&T subsequently benefited from retroactive immunity provided by the Foreign Intelligence Surveillance Act (FISA) Amendments Act of 2008.

According to the Congressional Research Service:

Although many of the changes enacted by the FISA Amendments Act were controversial, one particularly contentious issue was whether to grant retroactive immunity to telecommunications providers that may have facilitated warrantless surveillance by the federal government under a Terrorist Surveillance Program between 2001 and 2007.⁶

The issue has persisted in public attention and gained additional visibility in June 2013, when media reported that Edward Snowden leaked a court order showing that the NSA was collecting the telephone data records of millions of U.S. customers. Verizon was specifically known and named in the court order from the Foreign Intelligence Surveillance Court (FISC) as disclosing “telephony metadata.” FISC defines metadata as: “comprehensive communications routing information, including but not limited to session identifying information (originating and terminating telephone number, International Mobile Subscriber Identity Number, and International Mobile Station Equipment Identity Number), trunk identifier, telephone calling card number, and the time and duration of the call.”⁷ The strategy behind classifying the data collected as metadata is that metadata does not require a search warrant because it is not considered “communication....”⁸

Later media accounts also referenced similar involvement in the same program by AT&T.⁹

The elevation of metadata sharing to a subject of substantial public concern has been expressed by John Podesta of the Center for American Progress (recently appointed a senior advisor to President Obama):

...our smartphones with built-in GPS technology track our locations and our phone companies and Internet providers collect metadata on every call we make and every person we email. In the United States, court decisions from the pre-Internet days suggest that the information we give away voluntarily to these companies can be obtained fairly easily by the government. That legal rule may have made sense in an

⁵ Electronic Frontier Foundation, NSA Spying FAQ, <https://www EFF.org/nsa-spying/faq>.

⁶ <http://www.fas.org/spp/crs/intel/RL34600.pdf>

⁷ “NSA Files Decoded,” *The Guardian*, June 5, 2013. The documents released by Snowden indicate that the NSA runs these various surveillance programs through partnerships with major telecom companies.

⁸ Order of Judge Roger Vinson, In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from Verizon Business Network Services, Inc., on behalf of MCI Communication Services Inc, Docket No. BR 13-80, Foreign Intelligence Surveillance Court, page 2, “Telephony metadata does not include the substantive content of any communication, as defined by 18 U.S.C. § 2510(8).” See generally, the *Electronic Communications Privacy Act*, 18 U.S.C. §§ 2510–2522.

⁹ Siobhan Gorman, Evan Perez, & Janet Hook, *US Collects Vast Data Trove*, *Wall Street Journal*, June, 7, 2013, available at <http://online.wsj.com/article/SB10001424127887324299104578529112289298922.html> (reporting that AT&T also turns over call records pursuant to national security requests).

age before Facebook and iPhones, but we need a serious examination of whether it still makes sense today.¹⁰

AT&T Consumer Privacy Policy Revision and Controversy

In 2006, the Washington Post, CNN and a number of other major media outlets reported on changes AT&T made to its consumer privacy policy at that time, asserting ownership of certain customer related information. National Public Radio summarized:

AT&T is changing its privacy policy, *to show that some customer information belongs to AT&T*. Privacy advocates say the company is trying to protect itself against future lawsuits for helping government eavesdroppers. But AT&T says it simply updated its policy to reflect technological changes, and its recent merger.¹¹ [emphasis added]

That change in AT&T's privacy policy prompted widespread criticism from privacy advocates, including the Center for Democracy and Technology¹²:

This is bad news for consumers... AT&T is going to require customers to consent to the new policy as a condition of receiving service. The laws that prohibit phone companies from disclosing customer information to the government have exceptions for, among other things, *customer consent*. If AT&T were charged with improper disclosure of customer records to the government ... this change in policy would allow AT&T to claim that customers had consented to disclosure in order "to safeguard others" or to respond to "legal process."¹³

In 2009, AT&T revised its privacy policy again, prompting *The New York Times* to observe regarding the new policy:

It has a prominent section on location information, one of the biggest new types of information being collected by cellphone companies. It makes clear that AT&T knows where its cellphone customers are and uses that information to show ads for local merchants when they check yellow pages and use other services.

... And it explains how it tracks users of its Web sites and then can use that data to tailor ads to them on other sites...

... the company is saying more clearly than most other big companies that it knows a lot about you, that it will use that information to help it make more money in any number of ways, that it will keep the data for as long as you remain a customer, and

¹⁰ <http://www.spiegel.de/international/world/interview-with-obama-advisor-john-podesta-on-nsa-spying-scandal-a-913670.html>

¹¹ <http://www.npr.org/templates/story/story.php?storyId=5504560>

¹² <https://cdt.org/financialsdocs/CDT2011FundingbyCategory.pdf>

¹³ <https://www.cdt.org/blogs/nancy-libin/att-takes-big-step-back-privacy>

that it can be forced to give all that information to the government without giving you the chance to object.¹⁴ [emphasis added]

Drug Enforcement Administration/Hemisphere Project

Controversies surrounding the Company's involvement with government requests for information extend beyond its alleged participation in NSA-related programs. In 2013, *The New York Times* reported on a relationship between AT&T and the DEA that has existed since 2007:

For at least six years, law enforcement officials working on a counternarcotics program have had routine access, using subpoenas, to an enormous AT&T database that contains the records of decades of Americans' phone calls — parallel to but covering a far longer time than the National Security Agency's hotly disputed collection of phone call logs.

The Hemisphere Project, a partnership between federal and local drug officials and AT&T that has not previously been reported, involves an extremely close association between the government and the telecommunications giant.

The government pays AT&T to place its employees in drug-fighting units around the country. Those employees sit alongside Drug Enforcement Administration agents and local detectives and supply them with the phone data from as far back as 1987.¹⁵ [Emphasis added]

As with the news regarding the NSA, the revelations regarding the placement of AT&T staff in DEA offices seemed to go beyond the arms length relationship between the Company and government agents that consumers might expect.

Internet Company Transparency Reports

Consumer trust issues have arisen with the major internet companies on a parallel track with the telecoms. However, when faced with the controversy over government information requests, the major internet companies such as Google, Microsoft, Twitter, LinkedIn, Facebook and Yahoo!, have published such "Transparency Reports" disclosing information summarizing government data requests. For example:

- Google became the first major Internet company to issue a "Transparency Report" on requests "from governments and courts around the world to hand over user data in

¹⁴ Saul Hansel, *A New List of How Much AT&T Knows About You*, New York Times, June 11, 2009 http://bits.blogs.nytimes.com/2009/06/11/a-new-list-of-how-much-att-knows-about-you/?_r=0

¹⁵ Scott Shane, *Drug Agents Use Vast Phone Trove, Eclipsing NSA's*, September 1, 2013. <http://www.nytimes.com/2013/09/02/us/drug-agents-use-vast-phone-trove-eclipsing-nsas.html>

2010” and its website presents graphs of the number of user data requests, number of accounts impacted, and percentage of requests where some data is produced;¹⁶

- Microsoft issued its first transparency report (“2012 Law Enforcement Requests Report”) in March 2013¹⁷, detailing how “in 2012, Microsoft and Skype received a total of 75,378 law enforcement requests. Those requests potentially impacted 137,424 accounts. While it is not possible to directly compare the number of requests to the number of users affected, it is likely that less than 0.02% of active users were affected;”
- Facebook published its first transparency report (“Global Government Requests Report”) in August 2013, which states, “We scrutinize each request for legal sufficiency under our terms and the strict letter of the law, and require a detailed description of the legal and factual bases for each request. We fight many of these requests, pushing back when we find legal deficiencies and narrowing the scope of overly broad or vague requests;” and¹⁸
- Yahoo! published its first transparency report in September 2013, which details the total government requests, percentages and numbers of cases where data was disclosed, etc., and a link to the company’s Law Enforcement Response Guidelines.¹⁹

Many of these reports additionally describe the companies’ efforts to advocate for the protection of their clients’ data and privacy, and the specific actions taken to do so.

In July 2013, *TIME* noted a “dichotomy” between the actions of the major internet companies and telecommunications firms AT&T and Verizon:

As the U.S. National Security Agency scandal has unfolded over the last few weeks, internet giants Google, Facebook, and Yahoo have been falling over each other to publicly distance themselves from the NSA’s data collection programs, in some cases even going to a secret U.S. court to increase their transparency with the public. By contrast, the nation’s largest phone companies, including Verizon, AT&T, and Sprint, have remained stone-cold silent in the face of reports that they’ve participated in a vast, ongoing NSA data collection program targeting the phone records of tens of millions of Americans.²⁰

In August 2013, *TIME*’s headline was: “AT&T and Verizon Stay Silent About NSA Internet Snooping.”²¹

¹⁶ <http://www.google.com/transparencyreport/userdatarequests/>

¹⁷ <http://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/>

¹⁸ https://www.facebook.com/about/government_requests

¹⁹ <http://yahoo.tumblr.com/tagged/transparency>

²⁰ Sam Gustin, “NSA Scandal: As Tech Giants Fight Back, Phone Firms Stay Mum,” *Time*, July 3, 2013
<http://business.time.com/2013/07/03/nsa-scandal-as-tech-giants-fight-back-phone-firms-stay-mum/>

²¹ Sam Gustin, August 22, 2013,
<http://business.time.com/2013/08/22/att-and-verizon-stay-silent-about-nsa-internet-snooping/>

In September 2013, *TIME* reported: “Once again, the nation’s largest phone companies, including AT&T and Verizon Wireless, are absent from the push for greater transparency.”²²

Internationally, *The Guardian* stated (September 18, 2013):

America's top telecommunications companies are refusing to say whether they accept that the bulk collection of their customers' phone records by the National Security Agency is lawful....

The companies' decision not to comment on any aspect of the NSA dragnet puts them in a increasingly peculiar position. By withholding their internal views from the public, they are setting themselves apart from equivalent internet firms that are taking a more bullish stance, and are shrouding themselves in more secrecy than even the FISA court, one of the most tight-lipped institutions in the country.²³

The current Proposal is essentially a request to AT&T to engage in reporting on par with the transparency reports of the internet companies.

Disclosure of Wireless Customer Data

The concerns raised regarding the NSA, DEA and customer privacy policy changes have led to broader inquiry by policymakers on the Company's management of customer data.

On May 29, 2012, AT&T provided limited information about United States law enforcement demands for information about *wireless customers* in response to an inquiry by Congressman Ed Markey.²⁴ The Company's letter included information about the number of requests that the Company received from United States law enforcement for information about customers' wireless phone usage from 2007-2011, the types of requests received, and how many were denied. The Company also provided information about the amount of compensation it received for processing these requests for information about wireless customers, as well as other information about its policies and procedures related to law enforcement requests for wireless customer information.²⁵

On September 12, 2013, Markey (now a Senator) sent a follow-up letter to AT&T Communications with more detailed questions regarding mobile phone usage data requested

²² Sam Gustin, *Tech Titans Press Feds in Battle Over NSA Transparency*, September 10, 2013 <http://business.time.com/2013/09/10/tech-titans-press-feds-in-battle-over-nsa-transparency/>

²³ Ed Pickington, *Phone Companies Remain Silent Over Legality of NSA Data Collection*, September 18, 2013 <http://www.theguardian.com/world/2013/sep/18/phone-companies-silent-nsa-data-collection>

²⁴ AT&T's Response to Representative Edward J. Markey, May 29, 2012, available at http://www.markey.senate.gov/documents/2012-05-22_ATT_CarrierResponse.pdf.

²⁵ AT&T's Response to Representative Edward J. Markey, May 29, 2012, available at http://www.markey.senate.gov/documents/2012-05-22_ATT_CarrierResponse.pdf.

by law enforcement and national security requests under Section 215 of the Patriot Act.²⁶ AT&T sent a response to Senator Markey on October 3, 2013 and which was released publicly by the Senator on December 9, 2013.

Executive Action

President Obama, addressing concerns over NSA surveillance programs, earlier in 2013 said, “We can, and must, be more transparent. So I’ve directed the intelligence community to make public as much information about these programs as possible.” In August 2013, the U.S. Director of National Intelligence, James Clapper, announced that the intelligence community would publicly issue annual reports on certain surveillance requests.²⁷ Beyond just the total numbers of requests sent out, the report will also include the number of targets being investigated in each of the requests.

Presidential Review Group Issues Recommendations

President Obama commissioned the Review Group on Intelligence and Communications Technology (a special advisory committee) in August 2013 to make recommendations regarding the issues raised regarding national surveillance of telecom communications. The review group issued a report and recommendations to the President on December 12, 2013.²⁸

Among other things, the Review Group’s report, *Liberty and Security in a Changing World*,²⁹ recommends legislative action to authorize the telecommunication companies to publish summary data in transparency reports regarding FISA related communications.³⁰ It

²⁶ Senator Ed J. Markey letter to AT&T., Sept. 12, 2013, available at: http://www.markey.senate.gov/documents/2013-0912_Carrier_ATT.pdf

²⁷ Going forward the [Intelligence Community] will publicly release, on an annual basis, aggregate information concerning compulsory legal process under certain national security authorities. Specifically, for each of the following categories of national security authorities, the IC will release the total number of orders issued during the prior twelve-month period, and the number of targets affected by these orders:

- FISA orders based on probable cause (Titles I and III of FISA, and sections 703 and 704).
- Section 702 of FISA
- FISA Business Records (Title V of FISA).
- FISA Pen Register/Trap and Trace (Title IV of FISA)
- National Security Letters issued pursuant to 12 U.S.C. § 3414(a)(5), 15 U.S.C. §§ 1681u(a) and (b), 15 U.S.C. § 1681v, and 18 U.S.C. § 2709.

<http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/922-dni-clapper-directs-annual-release-of-information-related-to-orders-issued-to-telecom-providers-under-national-security-authorities>

²⁸ The recommendations were made public on December 18, 2013

²⁹ *Liberty and Security in a Changing World*, Report and Recommendations of The President’s Review Group on Intelligence and Communications Technologies, December 12, 2013.

³⁰ Recommendation number 9 of the Review Group report stated:

also proposes that the *telecommunication companies or third parties*, rather than the government, be tasked with retaining data on behalf of U.S. intelligence agencies, and conduct inquiries of that data on behalf of government, rather than delivering that data in bulk to government agencies.

On Tuesday, December 17, 2013, President Obama held a meeting with the CEOs of telecom and internet companies. Although the meeting was closed to the public, media reports reveal **that a significant focus of the meeting was on the impact on U.S. companies' business growth and opportunities caused by loss of confidence in privacy protection due to government information requests.**

The one topic the administration seemed most sympathetic to was the web companies' call for greater transparency around government surveillance requests, according to these people. It was the one issue nearly everyone in the room seemed most aligned on.³¹

Federal District Courts Issue Contradictory Rulings

In June 2013, a class action lawsuit was filed in the Federal District Court of Washington DC against Verizon, the U.S. Department of Justice, the NSA, President Obama and other high-level government officials. *Klayman v. Obama*. Civ. No. 13-0851 (RJL) (AT&T was recently added as a defendant.) The suit alleges that the companies' disclosure of and government access to customer data was illegal and criminal, violated constitutional rights, and caused the plaintiffs and class members mental and physical pain and suffering. The plaintiffs allege that the U.S. government's surveillance program constituted a violation of the First, Fourth and Fifth Amendments to the U.S. Constitution, violations of rights to privacy, due process and protection from intrusion upon seclusion.

The plaintiffs seek punitive damages in excess of \$3 billion. Plaintiffs also, as *Company Letter I* notes at page 5, seek "full disclosure and . . . accounting of what each

We recommend that legislation should be enacted providing that, even when nondisclosure orders are appropriate, recipients of National Security Letters, section 215 orders, pen register and trap-and-trace orders, section 702 orders, and similar orders issued in programs whose existence is unclassified may publicly disclose on a periodic basis general information about the number of such orders they have received, the number they have complied with, the general categories of information they have produced, and the number of users whose information they have produced in each category, unless the government makes a compelling demonstration that such disclosures would endanger the national security."

In the absence of such an enactment, some of the summary information requested under the current Proposal might be excluded from reports by the Company to the extent such disclosures are determined by the Company to be prohibited "subject to existing law."

³¹ http://www.nytimes.com/2013/12/18/us/politics/as-tech-industry-leaders-meet-with-obama-nsa-ruling-looms-large.html?_r=0

Defendant and government agencies as a whole have done and allowed the DOJ and NSA to do.”

The plaintiffs also seek declaratory, equitable and injunctive relief. On December 16, 2013, the court granted, in part, the plaintiffs’ motion for Preliminary Injunction, but stayed the order for six months pending appeal due to the “significant national security interests at stake” in the case. *Klayman v. Obama*, 1:13-cv-00851-RJL (D.D.C., Memorandum Opinion filed December 16, 2013). Judge Richard J. Leon, Federal District Court for the District of Columbia, noted:

“I cannot imagine a more ‘indiscriminate’ and ‘arbitrary’ invasion than this systematic and high-tech collection and retention of personal data on virtually every single citizen for purposes of querying and analyzing it without prior judicial approval... Surely, such a program infringes on ‘that degree of privacy’ that the founders enshrined in the Fourth Amendment.”

If the injunction becomes effective, it would end current NSA telecom provision of metadata and require erasure of the data from federal government records.³²

In contrast, in response to an ACLU challenge that focused on the constitutionality of the program,³³ another Federal District court (SDNY) in *ACLU v. Clapper* ruled on December 27, 2013 that the NSA metadata program was legal.

Thus, given the divergent opinions, it is apparent that these issues are likely to make their way through the appellate process en route to eventual resolution by the Supreme Court.

Recent Congressional Action

Sen. Al Franken, Chairman of the Judiciary Subcommittee on Privacy, Technology, and the Law, said, “Americans understand that we need to give due weight to privacy, on the one hand, and national security, on the other. But Americans are also naturally suspicious of executive power. And when the government does things secretly, Americans tend to think that power is being abused.” In the Senate, Sen. Franken (D-MN) and Sen. Dean Heller (R-NV) have co-sponsored and held hearings on the Surveillance Transparency Act of 2013. Among other things, the bill would make it easier for companies to report on government information requests.

³² The court’s preliminary injunction included (1) barring the Government from collecting, as part of the NSA’s Bulk Telephony Metadata Program, any telephony metadata associated with the plaintiffs’ Verizon accounts and (2) requiring the Government to destroy any such metadata in its possession that was collected through the bulk collection program. The court issued a six month stay of effectiveness of its ruling pending the government’s appeal, anticipated to ultimately reach the Supreme Court.

³³ <http://abcnews.go.com/US/wireStory/ny-judge-rules-nsa-phone-surveillance-legal-21348222>

In testimony, Sen. Heller highlighted the broad support in Congress for stronger transparency reporting: “The principles outlined in this bill to increase transparency for Americans and private companies would clear up a tremendous amount of confusion that exists with these programs. That is why transparency reform is included in multiple NSA reform proposals including the Intelligence Oversight and Surveillance Reform Act introduced by Senator Wyden, the USA FREEDOM ACT introduced by Chairman Leahy and myself, and the FISA Improvements Act introduced by Senator Feinstein.”

Similarly, in the House of Representatives, Rep. Zoe Lofgren (D-CA) and a bipartisan coalition have introduced a parallel effort, the Surveillance Order Reporting Act. The bill is being co-sponsored by Reps. Justin Amash (R-MI), Jason Chaffetz (R-UT), John Conyers (D-MI), Suzan DelBene (D-WA), Blake Farenthold (R-TX), Thomas Massie (R-KY), Jerrold Nadler (D-NY), Ted Poe (R-TX) and Jared Polis (D-CO).³⁴

ANALYSIS

1. The Proposal is not excludable as relating to ordinary business.

Long-standing SEC policy bars ordinary business exclusion of shareholder proposals addressing a significant policy issue.

The Company asserts in *Company Letter I* that the resolution is excludable because it relates to the Company's ordinary business operations. While Rule 14a-8(i)(7) permits companies to exclude from proxy materials shareholder proposals that relate to the company's ordinary business matters, the Commission recognizes that proposals relating to significant social policy issues transcend day-to-day business matters and raise issues so significant that they must be allowed to face a shareholder vote. The present Proposal is an exemplar of such a proposal.³⁵

³⁴ “The recent debate in Congress on these programs made it clear that we can't have an intelligent discussion on this issue without a more accurate grasp of the scope of surveillance,” said Rep. Lofgren. “This bill is a needed first step to free internet companies to provide the public information on how many surveillance orders they receive and how many of their users are affected.”

Rep. Justin Amash, a Republican co-sponsor of the House bill, told TIME magazine: “Businesses increasingly recognize that our government's out-of-control surveillance hurts their bottom line and costs American jobs. It violates the privacy of their customers and it erodes American businesses' competitive edge.”

³⁵ The SEC Staff explained that the general underlying policy of Rule 14a-8(i)(7) is “to confine the resolution of ordinary business problems to management and the board of directors, since it is impracticable for shareholders to decide how to solve such problems at an annual shareholders meeting.” SEC Release 34-40,018 (May 21, 1998). A proposal cannot be excluded under Rule 14a-8(i)(7) if it focuses on significant policy issues. As explained in *Roosevelt v. E.I. DuPont de Nemours & Co.*, 958 F. 2d 416 (DC Cir. 1992), a proposal may not be excluded if it has “significant policy, economic or other implications”. *Id.* at 426. Interpreting that standard, the court spoke of actions which are “extraordinary, i.e., one involving ‘fundamental business strategy’ or ‘long term goals.’” *Id.* at 427. Accordingly, for decades, the SEC has held that “where proposals involve business matters that are mundane in nature and do not involve any substantial policy or other considerations, the subparagraph may be relied upon to omit them.” *Amalgamated Clothing and Textile Workers Union v. Wal-Mart Stores, Inc.*, 821 F. Supp. 877, 891 (S.D.N.Y. 1993), quoting Exchange Act Release No. 12999, 41 Fed. Reg. 52,994, 52,998 (Dec. 3, 1976) (“1976 Interpretive Release”) (emphasis added).

The SEC clarified in Exchange Act Release No. 34-40018 (May 21, 1998) ("1998 Interpretive Release") that "Ordinary Business" determinations would hinge on two factors: whether the subject matter of the proposal addresses a significant policy issue for the company and whether the approach micromanages the company.

Subject Matter of the Proposal: "Certain tasks are so fundamental to management's ability to run a company on a day-to-day basis that they could not, as a practical matter, be subject to direct shareholder oversight. Examples include the management of the workforce, such as hiring, promotion, and termination of employees, decisions on the production quality and quantity, and the retention of suppliers. However, proposals relating to such matters but focusing on sufficiently significant social policy issues (e.g., significant discrimination matters) generally would not be considered to be excludable, because the proposals would transcend the day-to-day business matters and raise policy issues so significant that it would be appropriate for a shareholder vote." Exchange Act Release 34-40018 (May 21, 1998). ("1998 Interpretive Release").

"Micro-Managing" the Company: The Commission has also indicated that shareholders, as a group, will not be in a position to make an informed judgment if the "proposal seeks to 'micro-manage' the company by probing too deeply into matters of a complex nature upon which shareholders, as a group, would not be in a position to make an informed judgment." Such micro-management may occur where the proposal "seeks intricate detail, or seeks specific time-frames or methods for implementing complex policies." However, "timing questions, for instance, could involve significant policy where large differences are at stake, and proposals may seek a reasonable level of detail without running afoul of these considerations."

Recent Staff communications have indicated that the Staff uses several criteria in determining whether a matter *constitutes* a significant policy issue: level of public debate and controversy on the issue, media coverage, regulatory activity, legislative and Presidential involvement. In addition, the Staff considers whether the subject matter constitutes a new issue or if it has ripened into a lasting public concern. In addition, it is *also* necessary for the proponent to demonstrate a nexus of the policy issue to the company.

Finally, the Company bears the burden of persuasion on this question. Rule 14a-8(g). The SEC has made it clear that under the Rule "the burden is on the company to demonstrate that it is entitled to exclude a proposal." *Id.*

The subject matter, government requests for information from telecommunications companies, has ripened into a significant policy issue that transcends ordinary business.

In the present instance, the level of engagement by media, legislators, President Obama and the public on these issues of trust and transparency is exemplary of a significant policy issue.

An issue which is not treated by the Staff as a significant policy issue in one year may ripen into such an issue. Indeed, the Staff originally treated another subject matter facing the same companies, net neutrality, as excludable ordinary business for several years. With growth in congressional and media interest, the issue was determined by the Staff to have ripened into a significant policy issue in 2012. *Verizon Communications, Inc.* (March 2, 2010) and *Verizon Communications, Inc.* (March 12, 2010) (Division allowed exclusion of net neutrality proposal where Division “do[es] not believe [net neutrality] is a significant policy issue”); *AT&T, Inc.* (Feb. 10, 2012) (Exclusion as ordinary business rejected “in view of the sustained public debate over the last several years concerning net neutrality and the Internet and the increasing recognition that the issue raises significant policy considerations”).³⁶ With the present shareholder proposal, the same shift in treatment of the current subject matter is appropriate and necessary.

This is clearly a ripened issue. The Staff did not find a significant policy issue and allowed ordinary business exclusion in its prior rulings on proposals similar to the current one, - *AT&T Inc.* (Feb. 7, 2008), *Verizon Communications, Inc.* (Feb. 22, 2007), *AT&T Inc.* (Jan. 26, 2009).³⁷ However, the accumulated evidence *today* documents that this issue has attained the status of a high profile issue meeting all of the Staff’s criteria for a significant policy issue.

In its no-action request to the Staff, the Company asserts that concerns over its disclosure practices do not focus on a significant public policy issue for two reasons. First, the Company suggests that this is a short-term or perhaps passing issue of concern and debate, as the Company’s letter suggests “*this issue has not been seasoned by the test of time.*” *Company Letter 1*, page 7. However, as noted above in the background section, this issue has

³⁶ Net neutrality is the principle that all Internet service providers and governments should treat all data on the Internet equally. See e.g. the proposal underlying *AT&T, Inc.* (Feb. 10, 2012) requesting that AT&T “publicly commit to operate its wireless broadband network consistent with network neutrality principles - i.e., operate a neutral network with neutral routing along the company’s wireless infrastructure such that the company does not privilege, degrade or prioritize any packet transmitted over its wireless infrastructure based on its source, ownership or destination.”

³⁷ See e.g. the shareholder proposals underlying *AT&T Inc.* (Feb. 7, 2008), “RESOLVED: That shareholders of AT&T (the “Company”) hereby request that the Board of Directors prepare a report that discusses from technical, legal and ethical standpoints, the policy issues that pertain to disclosing customer records and the content of customer communications to federal and state agencies without a warrant . . .” and; *AT&T Inc.* (Jan. 26, 2009), “Therefore, be it resolved, that shareholders request the board issue a report by October 2009, excluding proprietary and confidential information, examining the effects of the company’s Internet network management practices in the context of the significant public policy concerns regarding the public’s expectations of privacy and freedom of expression on the Internet.”

occupied a great deal of public, media and congressional attention beginning at least as early as 2005. Furthermore, the recent recommendations of the Presidential Review Group ensure that this will continue to be controversial and a subject of debate for sometime to come.³⁸ A key recommendation of the review group would shift the duties of retaining and retrieving customer data from the NSA to the telecom companies or perhaps a third party:

In our view, the current storage by the government of bulk meta-data creates potential risks to public trust, personal privacy, and civil liberty. We recognize that the government might need access to such meta-data, which should be held instead either by private providers or by a private third party. This approach would allow the government access to the relevant information when such access is justified, and thus protect national security without unnecessarily threatening privacy and liberty.

Although it addresses the major issue of *NSA data collection, it also raises the prospect of continuing, or even expanding, the extent to which telecom arrangements with the government may undermine customer confidence in privacy protection.* The recommendations of the review panel, and the evolving relationship between national surveillance and telecommunication services, are likely to continue to be subject to high-profile debate for sometime to come. For instance the Washington Post reported reaction to the review group recommendation on December 25, 2013:

Civil libertarians consider mandated phone-company or third-party storage an unacceptable “proxy” for the NSA’s holding of the database. Last Thursday, a group of privacy advocates met with White House officials and urged them not to seek legislation to mandate data retention, among other things.

They endorsed an idea by a surveillance review group appointed by Obama to halt the NSA’s bulk storage of the phone logs. Although the panel did not recommend immediately requiring companies to retain the records, “that’s ultimately where the discussion is likely to lead,” said David Sobel, senior counsel for the Electronic Frontier Foundation, who raised the concern at the meeting. “That’s the obvious gorilla in the room.”

The phone companies, for their part, argue that storing the data for the NSA would lead to a flood of requests from local prosecutors, federal agents and divorce attorneys, unless legislation mandates it be used strictly for government counterterrorism purposes. Even then, the companies see it as a major headache.³⁹

³⁸ The President’s Review Group on Intelligence and Communications Technologies, *LIBERTY AND SECURITY IN A CHANGING WORLD*, December 12, 2013. http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

³⁹ http://www.washingtonpost.com/world/national-security/if-not-the-nsa-who-should-store-the-phone-data/2013/12/25/df00c99c-6ca9-11e3-b405-7e360f7e9fd2_print.html

Media coverage demonstrates a high level public controversy.

As documented in *Exhibit B* of this letter, this issue has drawn a high degree of interest from the media. Some examples include:

Zaroli, Jim, “Phone Companies Distance Themselves from NSA,” *National Public Radio*, May 16, 2006.

“AT&T Revises Privacy Policy,” *Los Angeles Times*, June 22, 2006.

Siobhan Gorman, Evan Perez, & Janet Hook, “U.S. Collects Vast Data Trove,” *The Wall Street Journal*, June 7, 2013.

Gustin, Sam, “Verizon, AT&T Challenged on NSA Spying,” *Time*, November 21, 2013.

Moritz, Scott, “AT&T Rejects Proposal to Report U.S. Requests for User Info,” *Bloomberg*, December 6, 2013.

Nakashima, Ellen, “Agencies collected data on Americans’ cellphone use in thousands of ‘tower dumps’,” *The Washington Post*, December 8, 2013.

Chen, Brian X, “A Senator Plans Legislation To Narrow Authorities’ Cellphone Data Requests,” *The New York Times*, December 9, 2013.

Gustin, Sam, “NSA Spying Scandal Could Cost U.S. Tech Giants Billions,” *Time*, December 10, 2013.

Cecilia Kang & Ellen Nakashima, “Tech Executives to Obama: NSA spying revelations are hurting business,” *The Washington Post*, December 17, 2013.

Savage, Charlie, “Judge Questions Legality Of NSA Phone Records,” *The New York Times*, December 17, 2013.

Evidence of the media's heightened interest in this issue is also well demonstrated by the fact that the Company's submission of a no-action request to the Staff itself elicited an unusual amount of attention and interest from national media including coverage of the letter in *The New York Times*, *Associated Press*, *Reuters*, *Bloomberg*, and *USA Today*.⁴⁰

⁴⁰ For instance, see http://bits.blogs.nytimes.com/2013/12/06/att-responds-to-shareholders-concerns-on-user-data/?_r=0; <http://www.bloomberg.com/news/2013-12-06/at-t-opposes-proposal-to-report-government-requests-on-user-info.html>; <http://www.usatoday.com/story/money/business/2013/12/06/att-says-it-doesnt-have-to-disclose-nsa-dealings/3894823/>.

Public interest in the issue is very substantial.

One measure often used by the SEC to assess the level of public concern and interest on an issue is the degree to which web searches or news searches turn up relevant articles. Google searches for articles on AT&T on December 18, 2013 revealed the following statistics indicative of a *very* high level interest in this issue. The searches included both searches under news stories only, and then more general Web searches using the following search criteria.

Search criterion: AT&T and Spying:

About 6,460 news story results

About 1,090,000 hits on default “web” search

Search criterion: AT&T and Snowden:

About 9,380 news story results

About 4,360,000 hits on default “web” search.

Search criterion: AT&T and NSA:

About 16,300 news story results

About 41,100,000 hits on default “web” search.

Search criterion: AT&T and Surveillance:

About 5,100 news story results

About 15,800,000 hits on default “web” search.

In addition to the degree of news coverage and web interest, surveys and citizen engagement on the issue provides additional evidence of public concern and interest. Surveys of the American public demonstrate that a majority of Americans do not feel current protections are adequate:

- A majority of Americans believe that the NSA is accessing both metadata and the content of their calls or emails from providers like AT&T⁴¹ and are especially concerned about cellular and wireless communications.⁴²
- A “clear majority” desire more Congressional oversight over the activities of the NSA⁴³ and many Americans believe that the government is infringing on civil liberties.⁴⁴

⁴¹ Timothy B. Lee, “Here is why ‘trust us’ is not working for the NSA anymore,” Wash. Post, July 30, 2013, <http://www.washingtonpost.com/blogs/the-switch/wp/2013/07/30/heres-why-trust-us-isnt-working-for-the-nsa-any-more/>.

⁴² <http://www.nytimes.com/2012/04/01/us/police-tracking-of-cellphones-raises-privacy-fears.html?pagewanted=all>

⁴³ <http://www.theguardian.com/world/2013/jun/13/nsa-surveillance-guardian-poll-oversight>

⁴⁴ <http://www.bloomberg.com/news/2013-07-10/snowden-seen-as-whistleblower-by-majority-in-new-poll.html>

- According to a survey by the Pew Research Center's Internet Project, asked whether they think current privacy laws provide reasonable protections for people's privacy on their online activities, 66% of all adults said the laws are "not good enough."⁴⁵

The nexus to the Company is clear.

In its request to the Staff, the Company asserts that "the debate in the press and before Congress has focused on proposals to reform the government's practices and the governing legal requirements, not on the disclosure practices of communications carriers with respect either to routine law enforcement requests or alleged court orders that mandate that they provide assistance to the government and that they not disclose that assistance."⁴⁶

That assertion is contradicted by the numerous media reports, domestically and internationally noted above, and examples of which are included with this letter in Appendix B, and by the actions of multiple members of Congress.⁴⁷ The *responses* of communications carriers to government information requests, as well as their apparent lack of legal resistance to those requests,⁴⁸ have been the subject of numerous news reports and analyses, as well as proposed legislation in the U.S. Senate and House of Representatives affecting the rights, liabilities and roles of the providers.

The role of AT&T and other telecommunication companies in compliance and cooperation with government information requests has been profiled by media as a specific business risk, potentially costing the Company billions of dollars in business, especially outside the United States.

Failure to persuade customers of a genuine and long-term commitment to privacy rights could present AT&T with serious financial, legal and reputational risks. This is especially true as the Company seeks to obtain consent from customers to ever increasing amounts of personal information. For instance, when the Company revised its privacy policy in June 2013, it informed its customers that unless they opted out, the Company would begin

⁴⁵ Anonymity, Privacy, And Security Online, (Pew Internet & American Life Project, Sept. 5, 2013), available at www.pewinternet.org/Reports/2013/Anonymity-online.aspx.

⁴⁶ Company Letter I, page 7.

⁴⁷ Senator Edward J. Markey (D-Mass.) has introduced legislation that does not focus on NSA or other intelligence agencies' programs, and would require a warrant to obtain GPS location data, impose limits on how long carriers can keep customers' phone data, and mandate routine disclosures by law enforcement agencies on the nature and volume of requests they make of carriers. Nakashima, Ellen, "Agencies collected data on Americans' cellphone use in thousands of 'tower dumps'," *The Washington Post*, December 8, 2013. See also Chen, Brian X, "A Senator Plans Legislation To Narrow Authorities' Cellphone Data Requests," *The New York Times*, December 9, 2013, discussing discrepancies among telecom companies in their data-sharing policies, records retention policies, and requirements of warrants versus subpoenas in responding to data requests, staff time dedicated to complying with requests and reimbursement for this work by the government.

⁴⁸ The declassified FISA Court opinion by Judge Claire V. Eagan revealed that no telecoms company has ever challenged the court's order for bulk collection of phone records and implied that by failing to challenge the legality of the program through legal means, such as an appeal, the phone companies were passively accepting its constitutional status. Pilkington, Ed. "Phone companies remain silent over legality of NSA data collection," *The Guardian*, September 18, 2013.

using location information... and website browsing and mobile application usage for “external marketing and analytics reports” on an aggregated and anonymous basis.⁴⁹

AT&T is no longer just a *phone* company. It is attempting to directly compete with many of the other technology companies in markets such as high speed internet delivery⁵⁰ and enterprise cloud services.⁵¹ AT&T reported in its quarterly report for the period ending in June 2013 that its “advanced business solutions” – “including VPN, Ethernet, hosting and other advanced IP services — grew more than 15 percent versus the year-earlier quarter. These services represent an \$8.4 billion annualized revenue stream.”⁵²

AT&T has stated that “for many customers our competitive advantage lies in our global network. We offer enterprise-grade network services in 182 countries representing 99 percent of the world’s economy.” Yet, AT&T’s international infrastructure and investments are vulnerable to the growing international concern about privacy and to international competition. The Information Technology and Innovation Foundation, a non-partisan research and educational institute promoting public policies to advance technological innovation and productivity,⁵³ estimated that disclosures regarding the NSA surveillance programs could cost the cloud computing industry \$21 billion to \$35 billion in lost business over the next three years if foreign customers decide the risks of storing data with a U.S. company outweigh the benefits.

The evidence and analysis gathered by media demonstrate that the Company is at risk of losing significant parts of these markets due to growing concerns about the extent to which the Company shares information about customers with the US government, leading to policy developments that could restrict its access to markets, especially internationally. As noted in the Proposal:

The Wall Street Journal has reported that AT&T’s plans to expand its mobile network in Europe, including anticipated acquisitions, could face “unexpected hurdles” due to its co-operation with NSA consumer information requests. ‘NSA Fallout Hurts AT&T’s Ambitions in Europe,’ October 30, 2013

⁴⁹ AT&T also stated it would begin serving advertisements to customers based on their location. AT&T Privacy FAQ: Questions About My Information & Advertising, <http://www.att.com/gen/privacy-policy?pid=13692#menu>. (“AT&T AdWorks uses information about the locations you visit in order to create combined wireless location interest characteristics that can be used to provide Relevant Advertising to you and others like you.”); Nicole Ozer, AT&T Wants Us to Pay Them With Our Money And Our Privacy—How to Opt Out, July 11, 2013, available at <https://www.aclu.org/blog/technology-and-liberty/att-wants-us-pay-them-our-money-and-our-privacy-how-opt-out>.

⁵⁰ Timothy J. Seppala, AT&T brings 300Mbps fiber internet to Austin in December, gigabit by ‘mid-2014’, engadget, Oct. 1, 2013, http://www.engadget.com/2013/10/01/att-uverse-austin-gigapower-got-the-ill-communication/?ncid=rss_semi

⁵¹ AT&T Synaptic Compute as a Service, AT&T.com, <http://www.business.att.com/enterprise/Service/cloud/computing/compute-as-a-service/>.

⁵² http://www.att.com/Investor/Earnings/2q13/ib_final_2q13.pdf

⁵³ www.itif.org

Also, *The Wall Street Journal* noted in June 2013:

Sen. Ron Wyden (D., Ore.), said he has warned about the breadth of the program for years, but only obliquely because of classification restrictions.

"When law-abiding Americans call their friends, who they call, when they call, and where they call from is private information," he said. "Collecting this data about every single phone call that every American makes every day would be a massive invasion of Americans' privacy."⁵⁴

In light of widespread, substantive and public evidence that the Company losing the trust of potential customers and current stakeholders, the nexus to the Company is clear.

The Proposal does not impermissibly relate to litigation.

The Company also asserts that the Proposal interferes with litigation to an extent that it should be excluded as ordinary business.⁵⁵ Because the Proposal does not interfere with litigation strategy, it is not excludable on this basis.

Only where a proposal would directly affect litigation strategy (*i.e.*, would require the registrant to divulge litigation strategy or to take affirmative action to concede a claim or defense in specific litigation) has the Division agreed that the proposal related to the "ordinary business" of the company. Proposals that rise to the level of "affecting the conduct" of litigation are those in which shareholders would direct their company as to how to act in litigation and/or explain litigation strategy. Mere existence of ongoing litigation does not provide a basis for the Staff to approve of the exclusion of a proposal under Rule 14a-8(i)(7). Numerous no-action letters rejecting exclusion bear this out. In *R.J. Reynolds Tobacco Holdings, Inc.* (March 7, 2000), the Division rejected exclusion where both the proposal and ongoing litigation addressed the Company's actions to prevent minors from accessing its tobacco products. The company had argued that although the proposal did not deal with matters relating to *whether* to institute legal proceedings, *how* the lawsuit ought to be conducted, or *whether* to settle a claim or appeal a judgment, *it was nonetheless excludable for proposing a course of action that was at issue in ongoing litigation*. The Staff rejected this argument. In *Dow Chemical* (February 11, 2004) and *Dow Chemical* (March 2, 2006) the Staff rejected Rule 14a-8(i)(7) exclusions of proposals requesting reports on new initiatives by the company to address health, environmental and social concerns of the Bhopal, India survivors, in spite of the presence of ongoing and potential future civil, criminal and administrative proceedings against the company related to environmental contamination in Bhopal.⁵⁶

⁵⁴ <http://online.wsj.com/news/articles/SB10001424127887324299104578529112289298922>

⁵⁵ *Company Letter I*, page 4.

⁵⁶ Many shareholder proposals touch upon the subject matter of litigation facing a company. In the absence of assertions that a given proposal represents an attempt to resolve a personal grievance (Rule 14a-8(i)(4)), the mere contemporaneity of a proposal with litigation related in substance does not make a proposal excludable. The Division has consistently rejected arguments that

The requirement for a proposal to directly affect litigation strategy in order to be excludable is demonstrated in each of the Staff letters cited by the Company: *Chevron Corp.* (Mar. 19, 2013) (Excluded proposal requested report on rationale for recent legal actions); *Merck & Co., Inc.* (Mar. 21, 2012) (Excluded proposal requested company file criminal charges and prosecute certain individuals); *NetCurrents, Inc.* (May 8, 2001) (Excluded proposal similarly required the company to initiate legal action); *Exxon Mobil Corp.* (Mar. 21, 2000) (Excluded proposal requested immediate payment of settlements). Each of these cases provides an example of shareholders impermissibly seeking to step into management's shoes and direct litigation strategy and decision-making. The present Proposal takes none of these impermissible actions.

This Proposal presents the opposite situation as *R. J. Reynolds Tobacco Holdings, Inc.* (Feb. 6, 2004), cited by the Company. In *R.J. Reynolds*, the proposal requested suspension of use of the terms "light," "ultralight" and "mild" to refer to the company's cigarettes. At the time, ongoing litigation sought the same remedy through an injunction prohibiting registrant from using "light" and "ultra light" in marketing. The proposal, if implemented, would have conceded the company's position in the ongoing litigation and thereby mooted the case. In contrast, here, the Proposal requests different information than what is at issue in litigation.

The Company states that it "has been a defendant in multiple pending lawsuits" "that generally allege that AT&T has violated customer privacy rights", yet the only case the Company refers to is *Klayman v. Obama*, Civ. No. 13-0851 (RJL) (D.D.C., complaint filed June 12, 2013).⁵⁷

The *Klayman* plaintiffs demand "full disclosure and . . . accounting of what each Defendant and government agencies as a whole have done and allowed the DOJ and NSA to do" in order to demonstrate the alleged illegality of the Defendants' actions.⁵⁸ The relief sought in *Klayman* is fundamentally different than the information sought in the present Proposal - implementation of the Proposal would not achieve the remedy sought by the plaintiffs in this case, nor aid in discovery in this case. In contrast, the Proposal seeks metrics of a much wider array of disclosures of government requests for information, in the U.S. and in other countries, well beyond the NSA issues. Reporting the metrics described in the

shareholder proposals improperly relate to litigation simply because the subject matter of the proposal was also the subject matter of litigation. For example, in *Philip Morris Companies, Inc.* (Feb. 14, 2000), shareholders sought a report on how the company intended to address health issues caused by their products. The company argued that the proposal improperly related to ongoing personal injury litigation against the company and should be excluded under Rule 14a-8(i)(7). The Division rejected this argument. See also *Philip Morris Companies, Inc.* (Feb. 22, 1999) (Division rejected argument that proposal requesting the company submit all future advertising to independent review to ensure that tobacco ads were not youth-friendly would impermissibly present a course of action that had the effect of dictating how the company will comply with its litigation settlement obligations to cease youth-friendly advertising).

⁵⁷ On December 16, 2013, the Court granted, in part, the Plaintiffs' motion for Preliminary Injunction, but stayed the order for six months pending appeal due to the "significant national security interests at stake" in the case. *Klayman v. Obama*, Civ. No. 13-0851 (RJL) (D.D.C., Memorandum Opinion filed December 16, 2013). If the injunction were to take effect it would have the effect of prohibiting the current NSA surveillance and erasure of the data from federal government records.

⁵⁸ Overall, the Plaintiffs seek declaratory, equitable and injunctive relief and punitive damages in excess of \$3 billion U.S. dollars, based in part on the alleged violation of Fourth Amendment rights by federal agents.

Proposal could not aid the *Klayman* plaintiffs in discovery, because it would be impossible to tell from these metrics whether any violation of constitutional rights, invasion of privacy, etc., had occurred in any particular instance. Furthermore, it would be impossible for the report requested by the Proposal to alter the course of the *Klayman* litigation because the language of the Proposal states that any report produced must be “subject to existing laws and regulation.” Since the Company’s interpretation of existing law is that current law requires *nondisclosure* of NSA information requests, the Company is apparently free to exclude information the *Klayman* plaintiffs might want from the requested report.⁵⁹

Finally, it seems a contradiction, at least, that the Company has now argued in *Company Letter II* that, unlike this asserted concern about affecting its litigation, its news release committing to issue a transparency report in the future should be treated as substantial implementation. If the Proposal were to interfere with litigation, it is hard to understand how the Company can also assert that it has implemented the Proposal, apparently without harm to its stance in litigation.

The Proposal does not overreach into matters of ordinary business.

The Company also asserts that the Proposal might be excluded as reaching into matters of ordinary business as well as matters of significant policy. Although the issue of responses to NSA information requests has been a catalyst for calling public attention to the extent to which the Company shares information with government entities, the information requested under the Proposal is as broad as necessary to encompass the concerns to shareholders raised by recent developments.

The various recent developments have generated a concern that government inquiries are *amoeba like*, extending their reach into customers’ data held by telecom company communications *from many directions at once*. Only a broad transparency report of the kind demonstrated in the Proposal can effectively address this concern and begin to restore trust. The Proposal concerns “requests for customer information by U.S. and foreign governments.” While one current cause for concern has been disclosures made by former NSA contractor Edward Snowden, the Proposal seeks to address the broader issue of customer trust that those disclosures have brought to public attention. The NSA metadata issues are only the tip of the iceberg.

The importance of this distinction was highlighted recently with the announcement by Sen. Ed Markey that federal, state and local law enforcement agencies collected data on

⁵⁹ However, if a legislative amendment such as that proposed on December 18, 2013 by the President’s Review Group on Intelligence and Communications Technologies is enacted as recommended by the President’s review committee, then the Company could become able to issue the requested report even for NSA related data. See The President’s Review Group on Intelligence and Communications Technologies, LIBERTY AND SECURITY IN A CHANGING WORLD, December 12, 2013. http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf. Even if the company were to issue such a report after such legislation is enacted, it would not substantially assist the litigation being pursued in *Klayman*.

hundreds or thousands of phone numbers of innocent Americans along with those of potential suspects through the use of so-called “tower dumps” from cell towers. As *The Washington Post* reported:

The little-known practice has raised concerns among federal judges, lawmakers and privacy advocates who question the harvesting of massive amounts of data on people suspected of no crime in order to try to locate a criminal. Data linked to specific cell towers can be used to track people’s movements.

The inquiry, by Sen. Edward J. Markey (D-Mass.), into law enforcement’s use of cellphone data comes amid growing scrutiny of the bulk collection of geolocation data overseas and of Americans’ phone records in the United States by the National Security Agency.

Note that Sen. Markey’s data was supplied by the major telecommunications carriers, including AT&T.⁶⁰

“This isn’t the NSA asking for information,” said Markey, who is planning to introduce legislation this month to restrict law enforcement’s use of consumers’ phone data, including ensuring that tower dumps are narrowly focused. “It’s your neighborhood police department requesting your mobile phone data. So there are serious questions about how law enforcement handles the information of innocent people swept up in these digital dragnets.”

Mr. Markey’s report received widespread media attention.⁶¹ AT&T’s eight-page letter to Sen. Markey provides data and analysis regarding law enforcement requests for information which may provide the basis for new legislation.

In addition to the cell phone surveillance, additional issues of surveillance and government information requests relevant and of concern to shareholders include evidence that the telecommunication companies have been collaborating with the U.S. government in spying on foreign leaders, which is spurring proposals for policy constraints on telecom company activities in Europe, Brazil, and elsewhere. These reports have also exacerbated the concern that customers in other countries may turn to competitors that are not plagued by these privacy concerns, and that policy or regulatory constraints may restrict AT&T’s access to those markets.

Furthermore, the Proposal does not impermissibly focus on the Company’s legal compliance programs. Although it addresses the issue of protection of consumer information, it is not focused on issues of legal compliance. For instance, it does not inquire as to

⁶⁰ http://www.markey.senate.gov/documents/2013-10-03_ATT_re_Carrier.pdf

⁶¹ e.g., <http://www.nytimes.com/2013/12/09/technology/a-senator-plans-legislation-to-narrow-authorities-cellphone-data-requests.html>

mechanisms or strategies that the Company utilizes to engage in legal compliance matters. The big picture statistics and discussion are built around the issues of restoring public and consumer trust rather than on the issues of compliance.

The Proposal specifically permits exclusion from the report, at the discretion of the Company, information about routine requests under individualized warrants. This latter category allows the Company the option of excluding many disclosures that it concludes might *only* relate to ordinary business and not to the broader issues of public and consumer trust. As AT&T seeks to expand its business models by directly competing with many of the other technology companies in new markets and further monetizing customer information, it becomes all the more important to the long term success of the business and the interest of shareholders for the Company to maintain the trust of customers by showing a strong commitment to privacy. Providing a top level review of how the Company is addressing these high profile issues of trust is no longer a matter of ordinary business; they “transcend the day-to-day business matters and raise policy issues so significant that it would be appropriate for a shareholder vote.”

2. The Proposal has not been substantially implemented and therefore cannot be excluded pursuant to Rule 14a-8(i)(10).

According to an AT&T news release of December 20, 2013:

To further our efforts to be as transparent as possible within the government guidelines in which we operate, like Verizon recently announced, we intend to publish a semi-annual online report that will provide information on the number of law enforcement requests for customer information that our company receives in the countries in which we do business. AT&T expects to publish the first report, covering information received in 2013, in early 2014.

To the extent permitted by laws and regulations, AT&T's transparency report will include:

1. The total number of law enforcement agency requests received from government authorities in criminal cases;
2. Information on the number of subpoenas, court orders and warrants;
3. The number of customers affected; and
4. Details about the legal demands AT&T receives, as well as information about requests for information in emergencies.

Finally, in our view, any disclosures regarding classified information should come from the government, which is in the best position to determine what can be lawfully disclosed and would or would not harm national security.

Company Letter II asserts that this news release promising the company's plans to issue transparency reports in the future should constitute “substantial implementation” of the

Proposal. Although this news release implies a *promise* to address portions of the Proposal, *promises* to produce a report do not constitute substantial implementation pursuant to Rule 14a-8(i)(10). *The J.M. Smucker Company* (May 9, 2011) (The Division disagreed with the company's assertion that its commitment to publish a sustainability report in the coming year acted as "substantial implementation" of a proposal requesting sustainability reporting). To allow a mere promise of action to serve as substantial implementation would be to create an enormous loophole under Rule 14a-8, allowing companies to preempt any shareholder proposal by issuing news releases reflecting a future intention to take requested actions. Shareholders whose proposals might be excluded on the basis of such promises would find they had no recourse if the promises are later broken.

None of the Staff precedents cited by the Company indicate an example where a proposal was allowed to be excluded based on a promise of future action. *Texaco, Inc.* (Mar. 28, 1991) (Proposal found excludable on reconsideration after company submitted extensive documentation of existing environmental programs, guidelines, assessment practices and more, that addressed the concerns of the proposal); *Anheuser Busch Cos., Inc.* (Jan. 17, 2007) (Proposal requesting shift to annual election of Directors was excludable where company had already declassified its Board and shifted to annual elections); *Exelon Corp.* (Feb. 26, 2010) (Proposal requesting disclosure of policies and procedures for political contributions and monetary and non-monetary political contributions excludable as moot after publication of new Corporate Political Contributions Guidelines document and issuance of report disclosing the Company's political contributions); *ConAgra Foods, Inc.* (July 3, 2006) (Proposal requesting issuance of sustainability report excludable as moot where company discussed sustainability in existing Corporate Responsibility Report); *Johnson & Johnson* (Feb. 17, 2006) (Proposal requiring the company and its U.S. subsidiaries to verify employment legitimacy of all current and future employees and immediately terminate any employee not authorized to work in the United States excludable where company was already legally required to take these actions and had done so); *Talbots Inc.* (Apr. 5, 2002) (Proposal requesting company implement code of conduct based on International Labor Organization human rights standards was excludable where company had existing standards, compliance programs and codes of conduct extensively addressing human rights).

The outcome would be different if, like the company in *Exelon Corp.* (Feb. 26, 2010) (cited above and by *Company Letter II*), the Company had actually issued the requested report, instead of merely promising to do so in the future. Exelon submitted a supplemental request for exclusion on February 19, 2010 and on the same date uploaded to the company website a *completed* report and *completed* guidelines that met the objectives of the underlying proposal. The Division thereafter found the proposal excludable as substantially implemented by this action.

In addition, the purported report, if it is issued based on the Company's specifications in the press release, it would not substantially implement the Proposal. The Company's press release describing its future transparency report limits the focus of reporting to government requests related to "criminal cases" only.

Media reports have cited “*millions*” of U.S. customers’ call records (metadata) reportedly provided to the U.S. government. It is highly unlikely that those “millions” of citizens were targeted in criminal cases. So, disclosures related to meta-data sharing with the NSA and any similar programs (for instance, sharing of cellular or land line metadata with state and local governments) would be excluded.

Similarly, many requests by foreign governments of information on political or religious dissidents’ phone calls, emails or calling records are outside of the scope of the Company’s intended report on criminal cases. It is not possible to enumerate or predict the range of *other* information that might be omitted by limiting the report to “criminal cases” only. However, as far as the Proponent can tell, absent production of the company’s “transparency report,” it would reflect only a small fragment of the disclosure requested by the Proposal. Further, it would fail to address its essential objectives of restoring public trust by providing transparency regarding the array of circumstances through which the Company fulfills government information requests. Thus, the Proposal is not excludable pursuant to Rule 14a-8(i)(10).

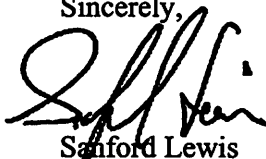
CONCLUSION

The Commission has made it clear under Rule 14a-8(g) that “the burden is on the company to demonstrate that it is entitled to exclude a proposal.” The Company has not met that burden that the Proposal is excludable under Rule 14a-8(i)(7) or Rule 14a-8(i)(10).

Therefore, we request that the Staff inform the Company that the SEC proxy rules require denial of the Company’s no-action request. In the event that the Staff should decide to concur with the Company, we respectfully request an opportunity to confer with the Staff.

Please call me at (413) 549-7333 with respect to any questions in connection with this matter, or if the Staff wishes any further information.

Sincerely,



Sanford Lewis
Attorney at Law

cc: Comptroller Thomas P. DiNapoli
Wayne A. Wirtz, AT&T
Patrick Doherty
Sen. Al Franken
Sen. Edward Markey

EXHIBIT A
Text of the Shareholder Proposal
Report on Government Requests for Consumer Information

Whereas,

Customer trust is critical for any business, but especially for major internet and telecommunications companies that routinely gather massive amounts of personal data concerning and affecting the lives of hundreds of millions of people in the U.S. and around the world.

The Wall Street Journal has reported that AT&T has provided millions of U.S. customers' call records to the U.S. National Security Agency (NSA). "US Collects Vast Data Trove," June 7, 2013.

AT&T acknowledges in its corporate code of conduct that privacy is critical to the success of its business. Yet, the Company has not disclosed to customers and investors any information regarding the extent and nature of requests for customer data made on the Company by government agencies.

Controversy over U.S. government surveillance programs reportedly involving AT&T has spurred massive global press coverage, hearings in the U.S. Congress and the European legislature, and widespread calls for reform. Brazilian President Dilma Rousseff called the NSA surveillance program "a breach of international law." U.S. Senator Ron Wyden said, "I have to believe the civil liberties of millions of Americans have been violated."

Responding to growing public concern over these issues, major internet companies such as Google, Microsoft, Twitter, LinkedIn, Facebook and Yahoo!, have published "Transparency Reports", disclosing information on government data requests. Google and Microsoft have also filed in court seeking authorization to disclose further information to the public concerning these requests. AT&T has not done so.

The Wall Street Journal has reported that AT&T's plans to expand its mobile network in Europe, including anticipated acquisitions, could face "unexpected hurdles" due to its co-operation with NSA consumer information requests. "NSA Fallout Hurts AT&T's Ambitions in Europe," October 30, 2013.

Transparency in this regard is essential if individuals and businesses are to make informed decisions regarding their personal data. Privacy is a fundamental tenet of democracy and free expression. While AT&T must comply with its legal obligations, failure to persuade customers of a genuine and long-term commitment to privacy rights could present AT&T with serious financial, legal and reputational risks.

Resolved, shareholders request that the Company publish semi-annual reports, subject to existing laws and regulation, providing metrics and discussion regarding requests for

customer information by U.S. and foreign governments, at reasonable cost and omitting proprietary information.

Supporting Statement: In preparing these reports, the Company may, at its discretion, omit information on routine requests provided under individualized warrants. The reports should be prepared with consideration of existing Transparency (or Law Enforcement Request) Reports published by the major internet companies, and where applicable, include such information as (1) how often AT&T has shared information with U.S. or foreign government entities; (2) what type of customer information was shared; (3) the number of customers affected; (4) type of government requests; and (5) discussion of efforts by the company to protect customer privacy rights.

EXHIBIT B
MEDIA COMPILATION

Bibliography

Zaroli, Jim. *Phone Companies Distance Themselves from NSA*.
National Public Radio. 5/16/2006.
<http://www.npr.org/templates/story/story.php?storyId=5409137>

From Bloomberg News. *AT&T Revises Privacy Policy*.
Los Angeles Times. 6/22/2006.
<http://articles.latimes.com/print/2006/jun/22/business/fi-privacy22>

From CDT.org. *AT&T Takes a Big Step Back on Privacy*.
Center for Democracy & Technology. 6/23/2006.
<https://www.cdt.org/blogs/nancy-libin/att-takes-big-step-back-privacy?issue=81>

Gorman, Siobhan; Evan Perez; Janet Hook. *U.S. Collects Vast Data Trove*.
The Wall Street Journal. 6/7/2013.
<http://online.wsj.com/news/articles/SB10001424127887324299104578529112289298922>

Frommer, Frederic J. *FISA judge: no challenges to phone records orders*.
The Big Story. 9/17/2013.
<http://bigstory.ap.org/article/fisa-judge-no-challenges-phone-records-orders>

Pilkington, Ed. *Phone companies remain silent over legality of NSA data collection*.
The Guardian. 9/18/2013.
<http://www.theguardian.com/world/2013/sep/18/phone-companies-silent-nsa-data-collection>

From RT. *NSA scandal may stop AT&T's ambitions to expand in Europe*. Russian Times.
11/1/2013. <http://rt.com/usa/nsa-att-telecom-vodafone-098/>

Gustin, Sam. *Verizon, AT&T Challenged on NSA Spying*.
Time. 11/21/2013.
<http://business.time.com/2013/11/21/verizon-att-challenged-on-nsa-spying/>

Moritz, Scott. *AT&T Rejects Proposal to Report U.S. Requests for User Info*.
Bloomberg. 12/6/2013.
<http://www.bloomberg.com/news/2013-12-06/at-t-opposes-proposal-to-report-government-requests-on-user-info.html>

Nakashima, Ellen. *Agencies collected data on Americans' cellphone use in thousands of 'tower dumps'*. The Washington Post. 12/8/2013.

http://www.washingtonpost.com/world/national-security/agencies-collected-data-on-americans-cellphone-use-in-thousands-of-tower-dumps/2013/12/08/20549190-5e80-11e3-be07-006c776266ed_story.html

Chen, Brian X. *A Senator Plans Legislation To Narrow Authorities' Cellphone Data Requests*. The New York Times. 12/9/2013.

Gustin, Sam. *NSA Spying Scandal Could Cost U.S. Tech Giants Billions*. Time. 12/10/2013.

<http://business.time.com/2013/12/10/nsa-spying-scandal-could-cost-u-s-tech-giants-billions/print/1/3/>

Kang, Cecilia; Nakashima, Ellen. *Tech Executives to Obama: NSA spying revelations are hurting business*. The Washington Post. 12/17/2013.

http://www.washingtonpost.com/business/technology/tech-executives-to-obama-nsa-spying-revelations-are-threatening-business/2013/12/17/6569b226-6734-11e3-a0b9-249bbb34602c_story.html

Savage, Charlie. *Judge Questions Legality Of NSA Phone Records*. The New York Times. 12/17/2013.

Nakashima, Ellen. *If not the NSA, who should store the phone data?*. The Washington Post. 12/25/2013.

http://www.washingtonpost.com/world/national-security/if-not-the-nsa-who-should-store-the-phone-data/2013/12/25/df00c99c-6ca9-11e3-b405-7e360f7e9fd2_story.html

Pages 74 through 82 redacted for the following reasons:

Copyrighted Material Omitted



All your cards.



One Coin. Pre-order now for \$50



The Big Story

FISA judge: no challenges to phone records orders

By FREDERIC J. FROMMER

— Sep. 17, 2013 8:17 PM EDT

[Home](#) » [Edward Snowden](#) » FISA judge: no challenges to phone records orders

WASHINGTON (AP) — A newly declassified opinion from the government's secret surveillance court says no company that has received an order to turn over bulk telephone records has challenged the directive.

The opinion by Foreign Intelligence Surveillance Court Judge Claire Eagan, made public Tuesday, spells out her reasons for reauthorizing the phone records collection "of specified telephone service providers" for three months.

The collection program, which the government says is authorized under Section 215 of the Patriot Act, was disclosed by former National Security Agency systems analyst Edward Snowden, provoking a heated debate over civil liberties.

Eagan had asked that her Aug. 29 opinion be made public "because of the public interest in this matter," and on Tuesday, the presiding judge of the FISA Court, U.S. District Judge Reggie Walton, ordered that the opinion be published. Portions of the opinion were blacked out.

"To date, no holder of records who has received an order to produce bulk telephony metadata has challenged the legality of such an order," wrote Eagan, who also serves on the U.S. District Court for the Northern District of Oklahoma, to which she was appointed by President George W. Bush. "Indeed, no recipient of any Section 215 order has challenged the legality of such an order, despite the explicit statutory mechanism for doing so."

She wrote that under Section 215 Congress provided for judicial review of FISA Court orders — first to the FISA Court of Review and, ultimately, to the U.S. Supreme Court. That provides for a "substantial and engaging adversarial process to test the legality of this court's orders under Section 215."

Eagan also concluded that the collection of phone records does not violate the Constitution's Fourth Amendment, which prohibits unreasonable search and seizure.

Verizon and T-Mobile US declined to comment on the opinion. AT&T and Sprint didn't return messages seeking comment.

The names of the companies the government is seeking the phone records from is blacked out in both the opinion and

order.

In another NSA data-collection program, PRISM, Yahoo is seeking to declassify a 2008 secret court order that required the company to turn over customer data to the government. In a filing with the court this year, Yahoo said disclosure of the opinion and briefs would allow the company to "demonstrate that it objected strenuously to the directives that are now the subject of debate, and objected at every stage of the proceeding," but that its objections were overruled. The Justice Department said last week it would declassify parts of that order.

Eagan also stressed in her opinion that prior to Congress reauthorizing Section 215 in 2011, the executive branch provided the intelligence committees of both the House and the Senate with detailed information about how the FISA Court was approving bulk telephone collection under the section. She said the executive branch worked with congressional committees to make sure that each member of Congress knew, or had the opportunity to know, how Section 215 was being implemented under the court's orders.

In a statement, Director of National Intelligence James R. Clapper said the opinion "affirms that the bulk telephony metadata collection is both lawful and constitutional. The release of this opinion is consistent with the president's call for more transparency on these valuable intelligence programs."

But Jameel Jaffer, deputy legal director of the American Civil Liberties Union, said that as a defense of the phone records collection program, the opinion is "completely unpersuasive."

Associated Press writer Stephen Braun contributed to this report.

Follow Fred Frommer on Twitter at <http://twitter.com/ffrommer>

Don't miss

- Snowden walks free in Russia to US anger
- SS United States is being prepared for a new life
- NSA collected thousands of US communications
- Ad3 Ways Guys Can Drop 20lbs QuicklyAd
- Ad15 NFL Cheerleaders Who Should Put on More ClothesAd
- Ad7 Healthy Foods that Turned Out to Be UnhealthyAd

Zemanta

Tags

Government and politics, North America, United States, Business, United States Congress, United States government, Legislature, Corporate legal affairs, Corporate news, Political issues, Social affairs, Social issues, Human rights and civil liberties, National governments, Government programs, Verizon Communications Inc, AT&T Inc, National courts, Courts, Judiciary, Reggie Walton, George W. Bush, Executive branch, Domestic spying, James R. Clapper, Jr., Edward Snowden, Government surveillance, Sprint Corp

Comments

Pages 85 through 86 redacted for the following reasons:

Copyrighted Material Omitted

theguardian

Search

Phone companies remain silent over legality of NSA data collection

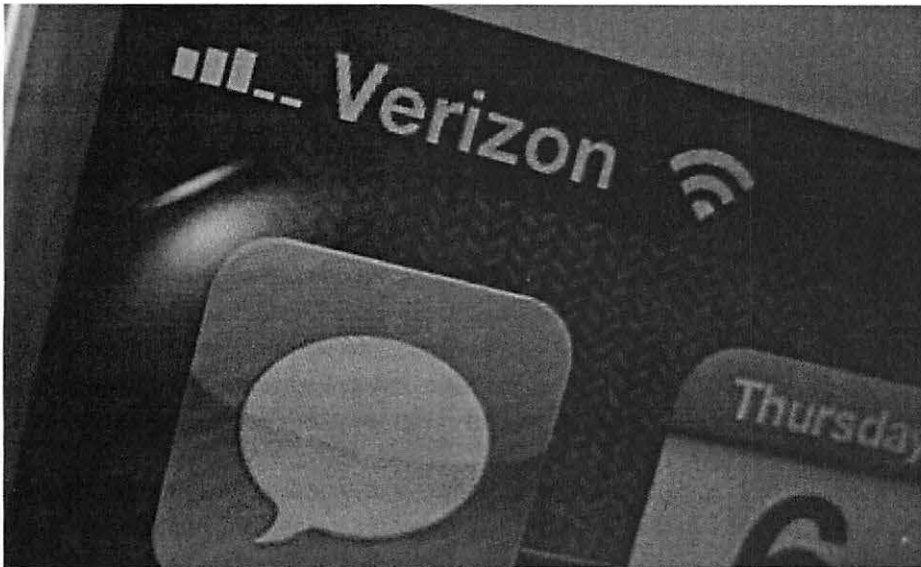
Leading phone firms refuse to say why they have not challenged Fisa court orders that compel them to hand over customers' data

Ed Pilkington in New York

Follow @edpilkington

Follow @guardian

theguardian.com, Wednesday 18 September 2013 16.23 EDT



Verizon was one of the companies that declined to answer Guardian questions over the legality of the NSA data collection. Photograph: Mike Blake/Reuters

America's top telecommunications companies are refusing to say whether they accept that the bulk collection of their customers' phone records by the National Security Agency is lawful.

The phone companies are continuing to guard their silence over the controversial gathering of metadata by the NSA, despite the increasingly open approach by those at the center of the bulk surveillance programme. On Tuesday the secretive foreign intelligence surveillance (Fisa) court declassified its legal reasoning for approving the NSA telephone metadata program periodically over the past six years.

Verizon, the telecoms giant that was revealed in June to be under a secret Fisa court order to hand over details of the phone records of millions of its US customers, was one of the firms that declined to answer Guardian questions relating to the legality of the scheme. AT&T, Sprint and T-Mobile US also declined to comment.

CenturyLink, a multinational company based in Monroe, Louisiana said: "At CenturyLink, we respect and protect the privacy of our customers and only provide information to the government when required or permitted by law. We do not comment on matters of national security or specific government requests for information."

In its declassified opinion, the Fisa court revealed that no telecoms company has ever challenged the court's order for the bulk collection of phone records. The opinion, written by Judge Claire V Eagan, implied that by failing to challenge the legality of the programme, the phone companies were passively accepting it its constitutional status.

Seeking clarification, the Guardian asked five of the top US telecoms firms whether their lack of resistance to the collection of their phone records was indeed an implicit acceptance of its legality.

The Guardian also asked how the phone companies could justify to their own customers the decision not to challenge the court orders, in stark contrast to some internet companies such as Yahoo, which have contested the legality of NSA collection of their customers' data.

The phone companies were asked by the Guardian to make clear whether they felt their compliance with Fisa court orders relating to NSA data collection was voluntary, or whether they felt pressured by any party into conceding without legal protest.

The companies' decision not to comment on any aspect of the NSA dragnet puts them in a increasingly peculiar position. By withholding their internal views from the public, they are setting themselves apart from equivalent internet firms that are taking a more bullish stance, and are shrouding themselves in more secrecy than even the Fisa court, one of the most tight-lipped institutions in the country.



Get the Guardian's daily US email

Our editors' picks for the day's top news and commentary delivered to your inbox each morning.

[Sign up for the daily email](#)

[Arabic](#) [Spanish](#) [Russian](#) [Freevideo](#) [IHOTB](#) [RTД](#) [RUPTLY](#)[Mobile apps](#)[RSS](#)

QUESTION MORE. LIVE

18:28 GMT, Dec 18, 2013

[News](#) [USA](#) [Russian politics](#) [Business](#) [Op-Edge](#) [In vision](#) [In motion](#) [Shows](#) [Bulletin board](#) [More](#)[Home](#) / [USA](#) /

NSA scandal may stop AT&T's ambitions to expand in Europe

Published time: November 01, 2013 20:42

[Get short URL](#)

AFP Photo / Etienne Franchi

[Like](#) 1.2k [Tweet](#) 146 [submit](#)[8+1](#) [Stun](#) 20

As leaks pertaining to secretive National Security Agency programs continue to surface, the international community at large is voicing concerns against the United States government. Now telecommunication providers could come under fire as well.

According to recent reports, an attempt by US-based telecom giant AT&T to acquire Europe's Vodafone company might be easier said than done as the unauthorized leaking of top-secret NSA documents continue to paint

Trends

NSA leaks

Tags

EU, Europe, Germany, Information Technology, Intelligence, Internet, USA

[Where to watch](#)[Schedule](#)[Follow us](#)

Recommended



Snowden ready to testify in Merkel tapping case – German lawmaker 101



Washington's answers don't justify NSA spying – EU delegation 19



NSA, 'Five Eyes' use Australian embassies to gather intel on Asia 30



not just the US intelligence agency in poor light, but also the private industry participants linked to the government's surveillance programs.

Earlier this week, the Wall Street Journal reported that AT&T's plan to expand on the other side of the Atlantic was being questioned after officials from Germany and other European nations voiced concern over the relationship between the US telecom and the NSA.

Should AT&T follow through with rumors to acquire Vodafone, the purchase would put the American company directly involved in one of the largest corporate acquisitions ever, the Journal reported. On the other hand, though, journalists with the magazine said, *"Europe's anger over the NSA's collection of electronic communications has reduced the likelihood a European deal could happen anytime soon."*

AT&T, along with Verizon and others, have been directly linked by NSA contractor-turned-leaker Edward Snowden as working in cahoots with government eavesdropping operations. Upon recent reports made possible through Snowden's disclosures in which it was detailed that the NSA snooped on the likes of German Chancellor Angela Merkel and even the Pope, European lawmakers may look towards limiting any possible deal between AT&T and an overseas entity such as Vodafone.

"One would really have to ask: Should this be allowed? Does this make sense? What does this mean for our standards of data privacy?" Anton Hofreiter of Germany's minority left-leaning Greens told the paper.

Peter Schaar, Germany's federal commissioner for data protection, added to WSJ that recent revelations could indeed sour any deal between AT&T and a European telecom.

"One would need to create transparency ahead of time so that everyone knows what the legal basis is" for how AT&T treats German data, he said. "The public and the regulators have become much more attentive now that we know, and also in part suspect, how far the surveillance goes."


And while Snowden leaks from earlier this week suggested that the NSA has been able to eavesdrop on countless people, American and otherwise, thanks to intricate surveillance programs, a spokesperson for the German ministry suggested such operations would be impossible — or at least illegal — if conducted overseas.

"Telecommunications companies that operate on German soil must hold



See offer
Shop
free sh


2-yr agreement with minimum monthly voice and data plans or Mobile Share plan required. While supplies last.



Snowden leak: NSA secretly accessed Yahoo, Google data centers to collect information 35



NSA chief calls reports about spying in France, Spain and Italy 'completely false' 82



POLITICKING
with Larry King

Thursdays
at 9pm EST

RT
AMERICA

themselves to German law," a spokeswoman said. "To transfer data to foreign intelligence agencies would be illegal."

Despite murmurings from German officials, though, others say the NSA may still be in the proper position to make an international acquisition. According to a report published Friday by Bloomberg News, Vodafone has been unable to thrive on its own as of late, and could benefit from a boost by AT&T. And as far as the US company is concerned, it might be a very opportune action.

"Buying Vodafone seems like an easy decision for AT&T given the value of their stock and the still-low interest rates," BTIG LLC New York analyst Walt Piecyk told Bloomberg.

Should the merger go through, Bloomberg's reporters say the new entity would bring together more than 400 million wireless subscribers across the world, and allow AT&T to compete directly with the likes of both Google and Apple. As outrage mounts internationally over the ongoing NSA scandal, though, the likelihood of any American company expanding operations overseas seems far from certain. Officials in Brazil have suggested that the country develop its own private internet to counter NSA surveillance, and authorities across Europe have compelled American representatives to explain allegations about spy operations targeting foreign leaders and civilians alike. Any acquisition made by an American company that would allow it to expand overseas is thus expected to come under increased scrutiny, and even mere murmurings of the potential AT&T/Vodafone deal could set the stage for regulators overseas to begin examining any newfangled relationships involving American telecom and tech companies.



Like

1.2k

Tweet

146



submit

8+1

Stun

20

Comments (4)

Ricardo Krachko 03.11.2013 15:17

EVERY NEW AMERICAN ENERGY JOB CREATES 3 MORE INDIRECT AND INDUCED JOBS.

SEE WHAT CHEVRON IS DOING >>



Human Energy

TECHNOLOGY & MEDIA

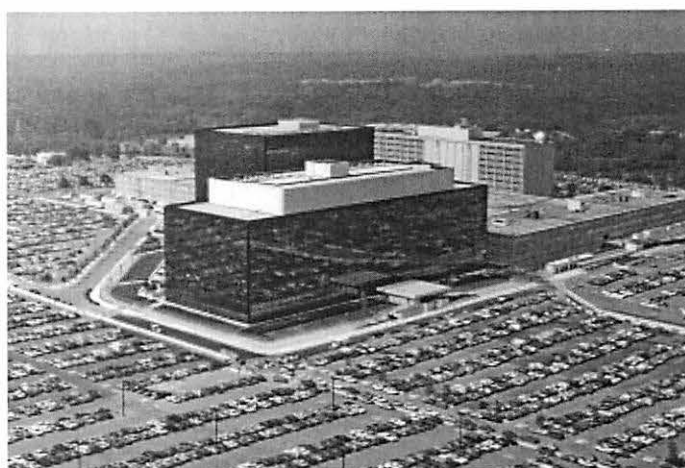
Verizon, AT&T Challenged on NSA Spying

Shareholders urge the telecom giants to be more transparent about U.S. data demands

By Sam Gustin @samgustin | Nov. 21, 2013 | Add a Comment

Verizon and AT&T, the nation's largest phone companies, have maintained a disciplined silence about their involvement with the U.S. government's controversial national security surveillance programs. Now, the telecom titans are facing pressure from influential shareholders to be more forthcoming about government requests for user information, including demands made by the National Security Agency (NSA) under the Foreign Intelligence Surveillance Act (FISA).

Shareholders are asking Verizon and AT&T to follow the example of the nation's largest Internet companies, including Google, Yahoo, Apple, Microsoft and Facebook, which all publish transparency reports. These companies are currently waging a legal battle with the government to be more forthcoming about government data demands. Internet and telecom firms alike are facing intense scrutiny following the blockbuster revelations from former NSA contractor Edward Snowden, who leaked classified documents describing the companies' participation in the NSA's



NSA / HANDOUT / REUTERS

The National Security Agency headquarters in Fort Meade, Md.

snooping programs.

The New York State Common Retirement Fund, which manages \$160.7 billion on behalf of more than one million state employees and retirees, is leading the effort for greater transparency. “AT&T’s failure to disclose what customer information it shares with U.S. and foreign governments presents significant risk to shareholder value,” said New York State Comptroller Thomas P. DiNapoli, trustee of the fund. “Transparency allows investors to make informed decisions about corporate behavior. Publishing regular reports on requests for information from governments would be an appropriate response to shareholder and customer concerns about trust and privacy in the digital world.”

(MORE: AT&T and Verizon Stay Silent About NSA Internet Snooping)

According to published reports, AT&T and Verizon, which control key points of the nation’s communications infrastructure, have worked with the NSA to install equipment that “copies, scans and filters large amounts of the traffic that passes through.” The telecom giants have installed the filtering equipment at more than a dozen key points throughout the nation’s communications grid. In 2006, a former AT&T technician revealed that the NSA had set up a monitoring point at an AT&T facility in San Francisco — the now-legendary Room 641A at 611 Folsom Street.

The purpose of the NSA’s surveillance programs is to collect “foreign intelligence” to prevent terrorist attacks against the United States and its allies. The systems are supposed to target people “reasonably believed” to be located outside the U.S., but recent revelations suggest that domestic communications have been collected. The NSA says that it has “minimization” procedures designed to ensure that U.S. citizens are not caught up in the government’s surveillance. But newly declassified documents show that the secret Foreign Intelligence Surveillance Court (FISC) has repeatedly criticized the U.S. for not following its own rules.

On a conference call with reporters in August, a senior U.S. intelligence official spoke in blunt terms about the cooperation of the telecom giants with the NSA surveillance programs. “The telecommunications companies are ordered to comply with this,” the official said. “That’s their role in this. As in a wide variety of other contexts, they get served with an order and they comply with the court’s order.” The official declined to either confirm or deny whether any of the telecommunications companies had ever objected to participating in the programs.

In another NSA program, authorized by the USA PATRIOT Act, the telecom giants work with the government to provide access to the phone records of tens of millions of U.S. citizens, including the number called, when the call was made, and the length of the conversation. Among the documents that Snowden leaked was a top-secret court order issued by the Foreign Intelligence Surveillance Court (FISC) — a secret court made up of 11 federal judges appointed by U.S. Chief Justice John Roberts — which requires Verizon to provide the NSA on an “ongoing, daily basis” with this so-called “metadata” on all phone calls made by its U.S. customers.

The shareholder groups are asking AT&T and Verizon to publish semi-annual reports — as the Internet companies do — “providing metrics and discussion regarding requests for customer information by U.S. and foreign governments, at reasonable cost and omitting proprietary information.” The proposals will be voted on at the companies’ annual meetings in Spring 2014.

AT&T spokesman Mark Siegel declined to address the substance of the shareholder proposal. “As standard practice we look carefully at all shareholder proposals but at this point in the process we do not expect to comment on them,” Siegel said. A spokesperson for Verizon did not immediately return a request for comment.

(MORE: Tech Titans Poised for Showdown With Justice Department Over NSA)

Verizon is being pressured by Trillium Asset Management, a Boston-based investment firm with more than \$1.3 billion under management. On its website, Trillium says that it integrates “environmental, social, and governance (ESG) factors into the investment process” as a way to identify good companies well positioned to deliver strong long-term performance.

“Verizon and AT&T are not managing this crisis effectively,” said Jonas Kron, SVP and director of shareholder advocacy at Trillium. “Now is the time for them to proactively demonstrate that they will protect user privacy, because it is in the interest of everyone —

investors, citizens, our nation and the companies. The business case is compelling – opportunities for growth may be lost – but equally important are the civil liberties that must be protected.”

Kevin Bankston, Policy Director of New America Foundation’s Open Technology Institute, urged AT&T and Verizon to join the effort to push for more transparency about the NSA’s surveillance programs. “The telcos failure to work with the privacy community to protect their users against government overreach, in contrast with the Internet companies who’ve joined our coalition, is especially disappointing considering that they are the ones who should be helping the most,” Bankston said.



Sam Gustin @samgustin

Sam Gustin is a reporter at TIME focused on business, technology, and public policy. A native of New York City, he graduated from Reed College and Columbia University's Graduate School of Journalism.

Bloomberg

AT&T Rejects Proposal to Report U.S. Requests for User Info

By Scott Moritz and Freeman Klopott - Dec 6, 2013

AT&T Inc. (T), the largest U.S. telephone company, opposes a shareholder resolution urging disclosures of government requests for customer information, calling it impracticable and an effort to “micromanage.”

AT&T, based in Dallas, said it guards its customers’ privacy, with protection entrusted to the company’s management, according to a Dec. 5 letter to the U.S. Securities and Exchange Commission.

New York State Comptroller Thomas DiNapoli and Trillium Asset Management LLC made the proposal last month. They’re urging more openness after reports this year that major Internet companies and U.S. carriers have cooperated with government agencies by sharing some customer data.

“AT&T is trying to prevent the vital issue of customer privacy from coming before its shareholders,” according to a statement from Eric Sumberg, a spokesman for DiNapoli’s office. DiNapoli is the trustee of the \$160.7 billion New York State Common Retirement Fund.

“This issue is an important one for customers and shareholders alike and we feel strongly that it should be on AT&T’s ballot this spring,” Sumberg said.

Verizon Communications Inc. (VZ), the second-largest U.S. telephone company, received a similar shareholder proposal last month from Trillium. Bob Varettoni, a Verizon spokesman, declined to comment.

In June, the Guardian newspaper reported on a secret court order directing New York-based Verizon to collect call data.

To contact the reporters on this story: Scott Moritz in New York at smoritz6@bloomberg.net; Freeman Klopott in Albany at fklopott@bloomberg.net

To contact the editor responsible for this story: Nick Turner at nturner7@bloomberg.net

Pages 96 through 97 redacted for the following reasons:

Copyrighted Material Omitted

The New York Times

Julia-Louis
Dreyfus

December 9, 2013

A Senator Plans Legislation to Narrow Authorities' Cellphone Data Requests

By BRIAN X. CHEN

SAN FRANCISCO — Cellphone carriers last year answered at least 1.1 million requests from law enforcement agencies seeking information on caller locations, text messages and other data for use in investigations, according to reports from the carriers.

Most of the requests were for information from a specific customer account. But law enforcement agencies also received information from 9,000 so-called tower dumps, in which the agencies were granted access to data from all the phones that connected to a cell site during a specified period of time.


The cellphone carriers' reports, which came in response to a congressional inquiry, underscored the law enforcement agencies' strong reliance on wireless phone records. The carriers are shown to turn over records thousands of times a day in response to police emergencies, subpoenas and other requests.

Senator Edward J. Markey, a Massachusetts Democrat, requested the reports from seven carriers, including AT&T, Verizon Wireless, Sprint and T-Mobile US. Mr. Markey conducted a similar audit last year as a member of the House, seeking information from carriers about law enforcement requests for 2011.

In 2011, the carriers complied with 1.3 million requests from law enforcement agencies. That number is not directly comparable with 2012's total of 1.1 million requests because Sprint, the third-largest American carrier, did not answer all of Senator Markey's questions.

Senator Markey said he planned to introduce legislation in the coming weeks that would provide stronger privacy protections for consumers, including the requirement of a warrant for police to get cellphone location information from a carrier as proof that it uncover evidence of a crime.

"Congress needs to ensure that our laws keep up with technology, including h enforcement handles and disposes of this sensitive mobile phone information



OPEN

MORE IN TE

**Spies' I
Playing
Trolls**

Read More

Markey said in a phone interview.

The wide-ranging nature of government surveillance programs, many of which have been revealed by documents leaked by Edward J. Snowden, has nudged some lawmakers to reassess the nation's privacy protections. Last week, it was reported that the N.S.A. tracks the location and movements of hundreds of millions of cellphones outside the United States, according to some of the documents leaked by Mr. Snowden.

Technology companies like Apple and Google have recently started publishing so-called transparency reports on the government and law enforcement requests that they receive, but the carriers have not released similar reports. The carriers' responses to Senator Markey about law enforcement requests are the closest thing yet to a transparency report.

The carriers sometimes resist requests from law enforcement, according to the reports. Reasons for rejection include when a request does not fully comply with the law — for example, when a signed court order is required instead of a subpoena. Verizon said in many instances law enforcement sought information that the carrier did not have.

But the carriers' responses to Senator Markey's inquiries also suggest that data-sharing policies are inconsistent among carriers. Some carriers, like AT&T and T-Mobile US, require a warrant for law enforcement to gain access to a person's current location data. But Verizon Wireless and Cricket say they cannot provide real-time location information at all.

The carriers also retain the location data collected from cell sites for varying periods of time. While most of the companies retain records for six to 18 months, AT&T holds them for five years.

Some types of content, like text messages or voice mail messages that are older than 180 days, are provided to law enforcement by AT&T with a subpoena, but not a warrant.

The carriers were also shown to comply with tower dumps at 9,000 cell sites, a small percentage of the 302,000 cell sites that were operational last year. But Christopher Calabrese, legislative counsel for the American Civil Liberties Union, who reviewed the carriers' responses, said the number of tower dumps was significant.

"Cell towers are handling hundreds of thousands of calls at any given time, getting personal info on hundreds of thousands of people for extended periods of time in order for police to gather information on one person," Mr. Calabrese said.

"What I was really struck by in looking at this stuff is the very powerful informants our

cellphones make,” he said. “They know so much about us and they can share so much about us — our texts, where we’re going online, our physical movements. It’s a host of information that clearly law enforcement is very aware of and actively accessing.”

The carriers devote a significant amount of resources to dealing with requests from law enforcement. For example, AT&T said in its response that it had a staff of 100 full-time employees working seven days a week handling responses. It received \$10.3 million in reimbursement for law enforcement responses last year.

Senator Markey said the legislation he planned to propose would require the Federal Communications Commission to limit the amount of time carriers could hold on to customers’ personal information. The senator said he also hoped to create a method to narrow down the information that police collected from a cell tower when doing so-called dumps.

Another piece of the legislation would require law enforcement officials to submit a signed and sworn statement whenever they received information from carriers in the case of emergency circumstances, to increase accountability for the requests. Senator Markey said he also wanted law enforcement to write routine reports disclosing the nature and volume of their requests.

INSIDE THE EMOTIONAL LIVES
OF BOYS [READ THE STORY NOW](#)

Apps

Business & Money

Economy | Wall Street | Tech | Small Business | Personal Finance | Real Estate | Business of Creativity | Management | Careers
New Energy

TECHNOLOGY & MEDIA

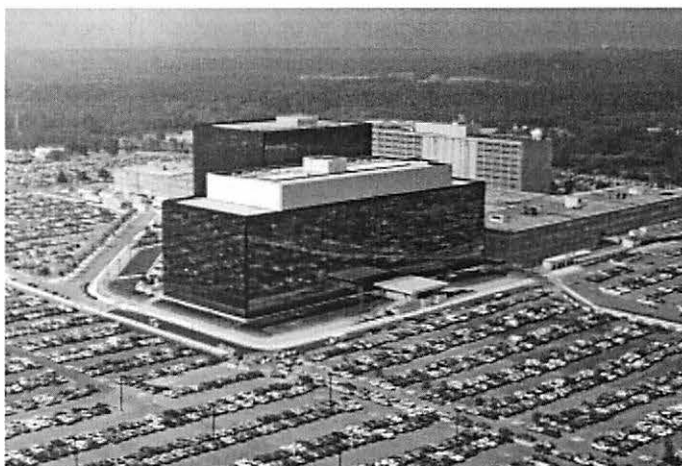
NSA Spying Scandal Could Cost U.S. Tech Giants Billions

AT&T and Verizon have remained silent about their role in the NSA's programs

By Sam Gustin @samgustin | Dec. 10, 2013 | 23 Comments

The National Security Agency spying scandal could cost the top U.S. tech companies billions of dollars over the next several years, according to industry experts. In addition to consumer Internet companies, hardware and cloud-storage giants like IBM, Hewlett-Packard, and Oracle could suffer billions of dollars in losses if international clients take their business elsewhere. Now, the nation's largest Internet companies are calling for Congress and President Obama to reform the U.S. government's secret surveillance programs.

Google, Apple, Microsoft, Yahoo, Twitter and Facebook are facing intense scrutiny following revelations from former NSA contractor Edward Snowden, who leaked classified documents about the NSA's snooping programs. In particular, the tech giants have been stung by disclosures about a classified U.S. intelligence system called PRISM, which the NSA used to examine data — including e-mails, videos and online chats — via requests made under the Foreign Intelligence Surveillance Act (FISA).



NSA / HANDOUT / REUTERS

The National Security Agency headquarters in Fort Meade, Md.

Snowden's disclosures stoked privacy concerns about how the largest U.S. tech companies handle their vast troves of user data. Since then, the companies have strenuously denied that they give the NSA "direct" or unfettered access to their computer servers, and they've waged a public competition to demonstrate their commitment to transparency. But recent reports have described how the NSA taps directly into the networks of the tech giants, a disclosure that prompted outrage from top company executives, most notably Eric Schmidt, Google's executive chairman.

(**MORE:** AT&T to Shareholders: No NSA Snooping Data for You)

After Snowden's leak, the Information Technology & Innovation Foundation (ITIF), a non-partisan, D.C.-based think tank, published a report saying that U.S. cloud computing providers could lose as much as \$35 billion by 2016 because of the NSA revelations. ITIF senior analyst Daniel Castro, the report's author, wrote that Snowden's disclosures "will likely have an immediate and lasting impact on the competitiveness of the U.S. cloud computing industry if foreign customers decide the risks of storing data with a U.S. company outweigh the benefits."

Analysts at Forrester, the respected tech industry research firm, went even further. In a blog post, Forrester analyst James Staten projected a net loss for the Internet service provider industry of as much as \$180 billion by 2016, which would amount to a 25% decline in the overall information technology services market. "All from the unveiling of a single kangaroo-court action called PRISM," Staten wrote. His estimate includes domestic clients, which could bypass U.S. cloud providers for international rivals, as well as non-U.S. cloud providers, which could lose as much as 20% of their business due to foreign governments — like Germany — which have their own secret snooping programs.

With numbers at that scale, it's not hard to understand why the top U.S. Internet companies are vehemently protesting the government's secret surveillance programs. Silicon Valley executives frequently tout their belief in idealistic principles like free speech, transparency and privacy. But it would be naive to think that they also aren't deeply concerned about the impact of the NSA revelations on the bottom line.

"Businesses increasingly recognize that our government's out-of-control surveillance hurts their bottom line and costs American jobs," Rep. Justin Amash, the Michigan Republican and outspoken critic of the NSA's secret programs, told TIME by email. "It violates the privacy of their customers and it erodes American businesses' competitive edge."

On Monday, a coalition of the largest U.S. Internet companies launched a campaign to pressure the government to reform its surveillance programs. "People won't use technology they don't trust," said Microsoft general counsel Brad Smith. "Governments have put this trust at risk, and governments need to help restore it." Several tech CEOs, including Google's Larry Page, Yahoo's Marissa Mayer and Facebook's Mark Zuckerberg, are personally throwing their weight behind the effort.

(MORE: NSA Scandal: As Tech Giants Fight Back, Phone Firms Stay Mum)

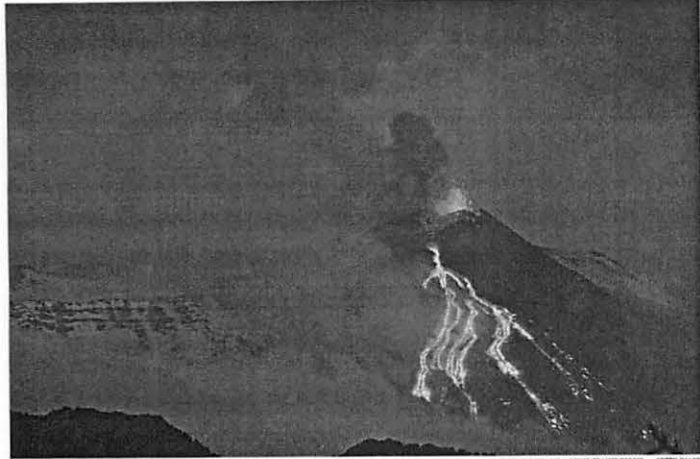
It's the most high-profile effort yet by the tech titans to repair the damage to their corporate reputations caused by the NSA revelations. The coalition is calling for limits on government authority to collect user information; better oversight and accountability; greater transparency about the government's demands; respect for the free flow of data across borders; and the avoidance of conflict between governments.

"Recent revelations about government surveillance activities have shaken the trust of our users, and it is time for the United States government to act to restore the confidence of citizens around the world," said Mayer, Yahoo's CEO. Page, Google's CEO, said: "The security of users' data is critical, which is why we've invested so much in encryption and fight for transparency around government requests for information. This is undermined by the apparent wholesale collection of data, in secret and without independent oversight, by many governments around the world."

Monday's statement by the leading Internet companies is the most forceful sign yet that they are serious about repairing the damage done to their reputations — and future business prospects — by the NSA revelations. But one group of companies that has also been implicated in the Snowden leaks remains conspicuously absent: The nation's largest telecom companies. Both AT&T and Verizon have remained stone-cold silent about their role in the NSA's programs. Last week, AT&T said it planned to ignore a shareholder proposal calling for greater transparency about government data requests.

The United States government is now at a crossroads. America faces difficult choices about how to balance the vital imperatives of national security and consumer privacy. For years, civil liberties groups warned that the Internet giants posed the greatest risk to privacy in the digital age. After the Snowden revelations, it's become clear that the gravest threat to civil liberties comes not from the private sector, but from the U.S. government itself. U.S. policymakers must decide if they wish to continue down the path toward an ever-more intrusive surveillance state — risking billions of dollars in damage to the U.S. economy — or apply real oversight and reform to an intelligence apparatus that has undermined confidence in the government and the nation's most innovative and profitable businesses.

Sam Gustin @samgustin



Fire on the Mountain; Hazard in the Air

Ash from Mount Etna, the volcano that has been erupting for weeks in Sicily, forced the island's busiest airport to close Monday.

Glaxo to Stop Paying Doctors To Boost Drugs

By KATIE THOMAS

The British drug maker Glaxo-SmithKline will no longer pay doctors to promote its products and will stop tying compensation of sales representatives to the number of prescriptions doctors write, its chief executive said Monday, effectively ending two common industry practices that critics have long assailed as troublesome conflicts of interest.

The announcement appears to be a first for a major drug company — although others may be considering similar moves — and it comes at a particularly sensitive time for Glaxo. It is the subject of a bribery investigation in China, where authorities contend the company funneled illegal payments to doctors and government officials in an effort to lift drug sales.

Andrew Witty, Glaxo's chief executive, said in a telephone interview Monday that its proposed changes were unrelated to the investigation in China, and were part of a yearslong effort "to try and make sure we stay in step with how the world is changing."

Continued on Page B2

A Political Deal in a Deeply Divided Tunisia

By CARLOTTA GALL

TUNIS — Compromise has been in short supply since Tunisia sparked the Arab Spring nearly three years ago. But this small North African nation has once again broken new ground with a political deal between longtime enemies among the Islamists and the secular old guard.

The deal, announced over the weekend, aims to put in place an independent caretaker government until new elections next year, marking the first time Islamists have agreed in the face of rising public anger to step back from power gained at the ballot box.

Tunisia had been careening toward chaos and political paralysis after two assassinations this year and an inability to finalize a new constitution, and it remains fragile and divided. But months of laborious back-room haggling helped, at least for now, to avoid the kind of zero-sum politics that have come to define the post-Arab Spring tumult in Egypt, Libya and the battlefield of Syria.

Beji Caid Essebbi, a former prime minister who leads a new secular-minded political party, Nidaa Tounes, and Rachid Ghannouchi, the leader of the Islamist party Ennahda, have starkly dif-

Islamists Agree to Step Back From Power in Crisis

ferent visions of the country's future. But since Tunisia's political crisis flared this year, the two men have met one on one at least five times to try to find a political solution.

It has not been easy for either side, and in an indication of just how deep the divisions remain, the two could still not agree on a candidate to serve as interim

prime minister. When the deal was announced late Saturday, between Ennahda and about half of the liberal parties in the opposition, Mehdi Jomaa, 50, the industry minister, was chosen as interim prime minister. But Mr. Essebbi did not sign on and could conceivably block cabinet picks.

Still, Ennahda was motivated to find a deal that would allow it to move forward with the framework the two men had worked out. Looking over its shoulder at the fall of President Mohamed Morsi in Egypt, and the crack-down on members of his Muslim Brotherhood that followed, the party was fearful of suffering the

Continued on Page A16

Judge Questions Legality Of N.S.A. Phone Records

Ruling Calls Program Arbitrary and 'Almost Orwellian,' but Allows Appeal

By CHARLIE SAVAGE

WASHINGTON — A federal district judge ruled on Monday that the National Security Agency program that is systematically keeping records of all Americans' phone calls most likely violates the Constitution, describing its technology as "almost Orwellian" and suggesting that James Madison would be "aghast" to learn that the government was encroaching on liberty in such a way.

The judge, Richard J. Leon of Federal District Court for the District of Columbia, ordered the government to stop collecting data on the personal calls of the two plaintiffs in the case and to destroy the records of their calling history. But Judge Leon, appointed to the bench in 2002 by President George W. Bush, stayed his injunction "in light of the significant national security interests at stake in this case and the novelty of the constitutional issues," allowing the government time to appeal it, which he said could take at least six months.

"I cannot imagine a more 'in-discriminate' and 'arbitrary' invasion than this systematic and high-tech collection and retention of personal data on virtually every single citizen for purposes of querying and analyzing it without prior judicial approval," Judge Leon wrote in a 68-page ruling. "Surely, such a program infringes on 'that degree of privacy' that the founders enshrined in the Fourth Amendment," which prohibits unreasonable searches and seizures.

Andrew Ames, a Justice De-

partment spokesman, said government lawyers were studying the decision, but he added: "We believe the program is constitutional as previous judges have found."

The case is the first in which a federal judge who is not on the Foreign Intelligence Surveillance Court, which authorized the once-secret program, has examined the bulk data collection on behalf of someone who is not a criminal defendant. The Justice Department has said that 15 separate judges on the surveillance court have held on 35 occasions that the calling data program is legal.

It also marks the first successful legal challenge brought against the program since it was revealed in June after leaks by the former N.S.A. contractor Edward J. Snowden.

In a statement from Moscow, Continued on Page A22

OBAMA'S LIBRARY, ADVISERS' DREAM

Loyalists and Locations Already Jockeying

By JASON HOROWITZ

WASHINGTON — This spring, a longtime staff member for President Obama, Alyssa Mastromonaco, let a friend in on a secret. Mr. Obama had assigned her to begin planning his post-presidential library and foundation.

It was a plum task. Amid a worsening crisis in Syria, early reports of ghosts haunting the HealthCare.gov machine and a dreary sense of second-term setbacks, the foundation glowed with the allure of an eternal Obama afterlife, or at least better days ahead. For Ms. Mastromonaco, the project promised the chance to shape a historic legacy and draft a road map for a 55-year-old former president's remaining life's work.

But a few weeks later, White House staff members noticed that an even greater force in the Obama orbit was moving toward the action. Valerie Jarrett, the first couple's matchmaker, early political patron and undisputed Obama whisperer, sensed a hot property.

The question of who guides Mr. Obama's next chapter may seem distant to the public. But, as aides to former President Bill Clinton have demonstrated, proximity to an ex-president translates into life at the intersection of wealthy donors, powerful networks and conference circuit perks. And with presidents departing the White House as relatively young men, there are many vying to bank in the Oval Office afterglow.

Early next year, Obama advisers are expected to announce a search for a home for Mr. Obama's foundation and library, a project that some of the president's closest financial supporters estimate could cost more than \$500 million.

The legacy project has proved magnetic to Obama liars both inside and outside the White House. Marty Nesbitt, a Chicago investor who is so close to Mr. Obama that he amounts to the effort's presidential seal of approval, is leading the outside campaign. He is working with the president's go-to fund-raiser and 2012 deputy campaign manager, Julianna Simon, to offer the first

Continued on Page A3

Boycott by Academic Group Is a Symbolic Sting to Israel

By RICHARD PÉREZ-PEÑA and JODI RUDOREN

An American organization of professors on Monday announced a boycott of Israeli academic institutions to protest Israel's treatment of Palestinians, signaling that a movement to isolate and pressure Israel that is gaining ground in Europe has begun to make strides in the United States.

Members of the American Studies Association voted by a ratio of more than two to one to endorse the boycott in online balloting that concluded Sunday night, the group said.

With fewer than 5,000 members, the group is not one of the larger scholarly associations. But its vote is a milestone for a Palestinian movement known as B.D.S., for Boycotts, Divestment and Sanctions, which for the past decade had found little traction in

the United States. The American Studies Association is the second American academic group to back the boycott, movement organizers say, following the Association for Asian American Studies, which did so in April.

"It's almost like a family betrayal," said Manuel Trajtenberg, a leading Israeli scholar. "It's very grave and very saddening that this happens, particularly so in the U.S.," he said.

Dr. Trajtenberg, an economics professor at Tel Aviv University, earned his doctorate at Harvard and has many Israeli academics as frequent sabbaticalists at American universities.

Israel has strong trade ties with Western Europe, where the B.D.S. campaign has won some backing for economic measures.

Continued on Page A4



Alain Leroy, owner of an auction company in Paris, surrounded by sacred Hopi spirit masks.

Secret Bids Guide Hopi Indians' Spirits Home

By TOM MASHBERG

The auction in Paris was set to move briskly, at about two items a minute; the room was hot and crowded, buzzing with reporters.

More than 100 American Indian artifacts were about to go on sale at the Drouot auction house, including 24 pieces, resembling masks, that are held sacred by the Hopi of Arizona. The tribe, United States officials and others had tried unsuccessfully to block the sale in a French court, arguing that the items were religious objects that had been stolen

many years ago.

Now the Ansenberg Foundation decided to get involved from its offices in Los Angeles. It hoped to buy all of the Hopi artifacts, plus three more sought by the San Carlos Apaches, at the Dec. 9 sale and return them to the tribes.

To prevent prices from rising, the foundation kept its plan a secret, even from the Hopis, in part to protect the tribe from potential disappointment. Given the nine-hour time difference, the foundation put together a team that could work well into the night, bidding by phone in the

auction in France.

The foundation had never done something like this before — a repatriation effort — and the logistics were tricky, to say the least.

Two staff members in Los Angeles, one a French speaker, were assigned to the job. The foundation also quietly arranged for a Paris lawyer, Pierre Servan-Schreiber, who had represented the Hopi pro bono in the court proceeding, to serve as lookout in the auction room.

He stood in the back, on the phone to the foundation. Whis-

Continued on Page A20

NATIONAL A18-23

Big Questions On Dinosaurs

A hobbyist reports a finding mistakes in research involving some of the world's top paleontologists.



PAGE A21

Antibacterial Soap Inquiry

The F.D.A. said that it would require manufacturers either to show the product was safe or stop making it.

PAGE A21

More Support for Budget Deal

A compromise plan now seems to have enough Republican votes to overcome a filibuster threat in the Senate.

PAGE A22

INTERNATIONAL A6-16

Pope Shakes Up Vatican Panel

Pope Francis replaced a conservative American cardinal on a powerful Vatican committee with another American considered more of a moderate.

PAGE A8

Thais See Too Much Democracy

Amid political upheaval in Thailand, a protest movement is standing up for less democracy, not more.

PAGE A8

SPORTS/TUESDAY B13-19

A Playbook on Brain Injuries

The National Institutes of Health outlined how it would use N.F.L. money for research on brain injuries.

PAGE B13

NEW YORK A24-27

An Afterlife For Artifacts

Closing churches send bells, statues and ritual objects to a warehouse on Staten Island for storage or for resale, to the clergy only.

PAGE A24

ARTS C1-8

A Shock, but No Thriller End

The "Homeland" finale had a shocking twist but, Alessandra Stanley says, it was even more startling that the story then carried on with a series of mundane details.

PAGE C1

BUSINESS DAY B1-11

Detecting a Shift by the Fed

The signs are growing that the Federal Reserve will soon taper off its bond-buying program and focus on other means to stimulate the economy.

PAGE B1

Whole Foods, Whole Nation

In its effort to expand, Whole Foods is finding success in smaller cities, in part by selling local goods.

PAGE B1

OBITUARIES B11-12

Ray Price Dies at 87

With his like "Crazy Arms," he made a revolutionary change in the beat of post-war country music.

PAGE B12

SCIENCE TIMES D1-8

Under Pressure, Some Surprises

When substances are pressed between two diamond anvils, familiar molecules transform — like oxygen into a shiny metal — a finding with implications for knowledge of the planet's core.

PAGE D1

EDITORIAL, OP-ED A28-29

Joe Nocera

PAGE A29



Tech executives to Obama: NSA spying revelations are hurting business



Video: President Obama discussed HealthCare.gov, intelligence leaks and the economy with leaders of technology companies on Tuesday.

By Cecilia Kang and Ellen Nakashima, [E-mail the writers](#) ↵

Leaders of the nation's biggest technology firms warned President Obama during a lengthy meeting at the White House on Tuesday that National Security Agency spying programs are damaging their reputations and could harm the broader economy.

The Washington Post

[Back to previous page](#)

Tech executives to Obama: NSA spying revelations are hurting business

By Cecilia Kang and Ellen Nakashima,
Published: December 17

Leaders of the nation's biggest technology firms warned President Obama during a lengthy meeting at the White House on Tuesday that National Security Agency spying programs are damaging their reputations and could harm the broader economy.

Cisco Systems has said it is seeing customers, especially overseas, back away from American-branded technology after documents revealed that the NSA enlisted tech firms and secretly tapped into their data hubs around the world as the agency pursued terrorism suspects. Companies such as IBM, AT&T and Verizon Communications are facing angry shareholders, some of whom have filed lawsuits demanding that the companies disclose their participation in NSA intelligence programs.

The companies also pressed the need for transparency and for limits on surveillance to restore the credibility of the U.S. government. They wanted an explanation of what the NSA was doing overseas to collect their data and to be able to talk about it, said industry and U.S. officials briefed on the meeting who spoke on the condition of anonymity to discuss it freely.

"Most companies" in the room pressed this point, "and they did so loudly," said one U.S. official.

Obama said that he heard their message and that the White House would consider the group's views as it completed a review of NSA surveillance programs.

Silicon Valley has been a critical driver of the economic recovery and has long represented the face of American ingenuity around the world. Many of these companies say they are still trying to assess the damage caused by Edward Snowden's leak of NSA documents showing their work with intelligence officials.

But some shareholders say Silicon Valley has been slow to recognize the reputational crisis that is developing around the world for these companies. "Verizon and AT&T are not managing this crisis effectively," said Jonas Kron, director of shareholder advocacy at Trillium, an investment advisory firm.

“Now is the time for these companies to demonstrate that they will protect user privacy.”

The morning meeting at the White House, held in the Roosevelt Room, took on added import given a federal judge’s ruling Monday that the NSA’s counterterrorism program to collect Americans’ phone records appears to be unconstitutional. That, along with the outcry from Silicon Valley and civil liberties advocates, some of whom belong to Obama’s party, is increasing pressure on the administration to curb NSA surveillance efforts.

The gathering was scheduled for two hours but went well over the allotted time, with the majority of the discussion focused on the companies’ demands for changes to NSA spying programs, according to tech industry officials.

Several of the executives came to the meeting particularly angered over a Washington Post report in late October that revealed the NSA and its British counterpart, Government Communications Headquarters, or GCHQ, were gaining access to the data connections that link Google and Yahoo servers around the world, industry officials said.

Their message was to say: “What the hell are you doing? Are you really hacking into the infrastructure of American companies overseas? The same American companies that cooperate with your lawful orders and spend a lot of money to comply with them to facilitate your intelligence collection?” said one industry official familiar with the companies’ views.

The NSA has stressed that its overseas collection is carried out lawfully, under executive authority. Any data on Americans are handled according to rules that protect their privacy, including the requirement to obtain a warrant to target an American’s communications, officials say.

In the meeting, the executives reiterated a list of demands that had been sent to the White House in a letter last week calling on the administration to cease bulk data collection of e-mails, online address books and other personal information; to impose limits on how easily the NSA can obtain court orders for Internet data; and to allow the companies to be more transparent about government intelligence requests.

Several participants acknowledged that the White House had to balance the companies’ business concerns against national security considerations.

Senior administration officials described the meeting with the 15 executives as “constructive, not at all contentious.”

“This was an opportunity for the President to hear from CEOs directly as we near completion of our review of signals intelligence programs, building on the feedback we’ve received from the private sector in recent weeks and months,” the White House said in a statement.

One participant suggested the president pardon Snowden. Obama said he could not do so, said one industry official. White House officials have said that Snowden is accused of leaking classified information and faces felony charges in the United States, and that he should be returned as soon as possible to the United States, “where he will be accorded full due process and protections.”

Senior executives from AT&T, Yahoo, Apple, Netflix, Twitter, Google, Microsoft and Facebook were among those in attendance.

“We appreciated the opportunity to share directly with the President our principles on government

surveillance that we released last week and we urged him to move aggressively on reform,” the technology firms said in a joint statement after the meeting.

Many of these firms have played a key role in boosting Obama’s political fortunes. Tech companies pumped nearly \$7.8 million into his campaign in the last cycle, according to the nonpartisan Center for Responsive Politics.

Some of the top officials meeting with the president Tuesday served as bundlers for his 2012 bid. Yahoo’s chief executive, Marissa Mayer, raised between \$100,000 and \$200,000, according to the center, and Shervin Pishevar, co-founder of the Sherpa technology investment fund, raised more than \$500,000. Mark Pincus, Zynga’s chief product officer and chairman, gave \$1 million to Priorities Action USA, the super PAC that supported Obama.

Still, some of these executives, as well as their shareholders, are fretting about the bottom-line impact of the NSA intelligence programs.

In Cisco’s earnings report last month, executives explained that disappointing sales in emerging markets were partly tied to the NSA leaks, which may have “caused a number of customers to pause and reevaluate,” Cisco’s head of sales, Robert Lloyd, said at the time.

Last week, IBM shareholders sued the company in a New York federal court, saying that it harmed investors with its secret participation in NSA programs.

“IBM’s association with the NSA presented a material risk to the company’s sales and, in particular . . . sales in China that were of critical importance to investors,” the Louisiana Sheriffs’ Pension and Relief Fund said in its lawsuit. “Despite that knowledge . . . IBM misrepresented to investors that it was a market leader in the Asia-Pacific region and that IBM expected solid improvement in the sales of its hardware division.”

Last month, shareholders of Verizon and AT&T demanded that the companies disclose their participation in NSA intelligence programs.

The \$160.7 billion New York State Common Retirement Fund filed a resolution with AT&T’s board to make public its participation in government intelligence programs. The pension fund argued that customers can too easily switch to another wireless carrier amid concerns that AT&T is sharing telephone data and other information with the government.

The meeting at the White House was the second time top Silicon Valley and telecommunications leaders have convened with Obama since Snowden began to release portions of a trove of top-secret documents detailing NSA spying programs.

Obama tried to keep the tenor friendly, even cracking jokes, an industry official said.

At one point, he asked Netflix chief executive Reed Hastings if he brought advanced copies of the second season of “House of Cards,” a satire-drama of Washington politics, according to a pool report of the meeting.

Hastings laughed and invited Obama to do a cameo appearance on the show. Obama said of the ruthless lead character, a congressman played by Kevin Spacey, “This guy’s getting a lot of stuff done.”

Pages 108 through 110 redacted for the following reasons:

Copyrighted Material Omitted



Wayne A. Wirtz
Associate General Counsel
208 S. Akard, Room 3024
Dallas, Texas 75202
(214) 757-3344
ww0118@att.com

1934 Act/Rule 14a-8

By email to shareholderproposals@sec.gov

December 27, 2013

U.S. Securities and Exchange Commission
Division of Corporation Finance
Office of Chief Counsel
100 F St., NE
Washington, DC 20549

Re: AT&T Inc. – Supplemental Request to Exclude Shareholder Proposal of the New York State Common Retirement Fund et al.

Ladies and Gentlemen:

On December 5, 2013, AT&T Inc., a Delaware corporation (“AT&T” or the “Company”), submitted a letter stating its intent to exclude from its proxy statement and form of proxy for its 2014 Annual Meeting of Shareholders (collectively, the “2014 Proxy Materials”) a shareholder proposal (the “Proposal”) and statement in support thereof (the “Supporting Statement”) submitted by the New York State Common Retirement Fund and co-filers Sarah Nelson, Louise Rice, Tamara Davis, John Silva and Shana Weiss (collectively, the “Proponents”). In light of a new development, we are supplementing our December 5, 2013 letter to add a separate argument to exclude the Proposal pursuant to Exchange Act Rule 14a-8(i)(10) – substantial implementation.

ARGUMENT

The Proposal May Be Excluded Pursuant to Exchange Act Rule 14a-8(i)(10).

On December 20, 2013, AT&T issued a press release announcing its intent to publish a Transparency Report disclosing law enforcement requests for customer information that AT&T received in 2013 in the United States and the other countries in which it does business (the “AT&T Transparency Report”). A copy of the press release is attached to this letter as Exhibit A. As stated in the press release, AT&T expects to publish its first AT&T Transparency Report in early 2014 and to update it semi-annually. The AT&T Transparency Report will include, to the extent permitted by laws and regulations:

- The total number of law enforcement agency requests received from government authorities in criminal cases;
- Information on the number of subpoenas, court orders and warrants;
- The number of customers affected; and
- Details about the legal demands AT&T receives, as well as information about requests for information in emergencies.

The Proposal requested that “the Company publish semi-annual reports, subject to existing laws and regulation, providing metrics and discussion regarding requests for customer information by U.S. and foreign governments, at reasonable cost and omitting proprietary information.” The Supporting Statement provides that this report “should be prepared with consideration of existing Transparency (or Law Enforcement Request) Reports published by the major internet companies, and where applicable, include such information as (1) how often AT&T has shared information with U.S. or foreign government entities; (2) what type of customer information was shared; (3) the number of customers affected; (4) type of government requests; and (5) discussion of efforts by the company to protect customer privacy rights.”

Rule 14a-8(i)(10) permits a company to exclude a proposal from its proxy materials if the company “has already substantially implemented the proposal.” For a proposal to have been acted upon favorably by management, it is not necessary that the proposal have been implemented in full or precisely as presented. *See* Release No. 34-20091 (Aug. 16, 1983). Instead, “a determination that the company has substantially implemented the proposal depends upon whether [the company’s] particular policies practices and procedures compare favorably with the guidelines of the proposal.” *Texaco, Inc.* (Mar. 28, 1991). In other words, substantial implementation under Rule 14a-8(i)(10) requires a company’s actions to have satisfactorily addressed both the proposal’s underlying concerns and its essential objective. *See Exelon Corp.* (Feb. 26, 2010); *Anheuser Busch Cos., Inc.* (Jan. 17, 2007); *ConAgra Foods, Inc.* (July 3, 2006); *Johnson & Johnson* (Feb. 17, 2006); *Talbots Inc.* (Apr. 5, 2002).

The AT&T Transparency Report substantially implements the Proposal because it will contain information that compares favorably with the information requested by the Proposal and it satisfies the Proposal’s essential objective. The AT&T Transparency Report will be published semi-annually, as requested by the Proposal; it will disclose the total number of law enforcement agency requests received from government authorities in criminal cases, which satisfies “(1) how often AT&T has shared information with U.S. or foreign government entities”; it will disclose the number of customers affected, which satisfies “(3) the number of customers affected”; and it will disclose the number of subpoenas, court orders and warrants, including details about the legal demands AT&T receives, as well as information about requests for information in emergencies, which satisfy “(4) type of government requests”. AT&T’s Privacy Policy¹ and Code of Business Conduct² already discuss the Company’s efforts to protect customer privacy

¹ *See* AT&T Privacy Policy (available at <http://www.att.com/gen/privacy-policy?pid=2506>).

² *See* AT&T Code of Business Conduct (available at: http://www.att.com/Common/about_us/downloads/att_code_of_business_conduct.pdf).

rights, which satisfy "(5) discussion of efforts by the company to protect customer privacy rights."

Out of the five categories of information specified in the Proposal, the only category that the AT&T Transparency Report will not address is "(2) what type of customer information was shared." However, none of the Transparency or Law Enforcement Request Reports issued by Google, Microsoft, Twitter, LinkedIn, Facebook and Yahoo! disclose this type of information either, and the Supporting Statement states that AT&T's report "should be prepared with consideration of existing Transparency (or Law Enforcement Request) Reports published by the major internet companies."


We recognize that the AT&T Transparency Report has yet to be issued, and will not be issued until early 2014. However, we submit that the public commitment by AT&T to issuing this report, as announced in the December 20, 2013 press release, and the specific types of information that AT&T has announced in the press release will be included in this report substantially implement the Proposal's objective. After all, the Proposal contemplates that a report would be issued in the future. The general policy underlying the basis for exclusion under Rule 14a-8(i)(10) is "to avoid the possibility of shareholders having to consider matters which have already been favorably acted upon by the management." Release No. 34-12598 (July 7, 1976). As AT&T has publicly committed to issuing the AT&T Transparency Report and its Privacy Policy and Code of Business Conduct are available on AT&T's website, the Proposal has already been favorably acted upon by management, and there would be little purpose in having the Proposal voted on by shareholders at the 2014 Annual Meeting.

CONCLUSION

Based upon the foregoing analysis, in addition to the arguments set forth in our December 5, 2013 letter, we respectfully request that the Staff concur that it will take no action if the Company excludes the Proposal from its 2014 Proxy Materials.

We would be happy to provide you with any additional information and answer any questions that you may have regarding this subject. Correspondence regarding this letter should be sent to me at ww0118@att.com. If I can be of any further assistance in this matter, please do not hesitate to contact me at (214) 757-3344.

Sincerely,


Wayne Wirtz

Attachment: Exhibit A

cc: Patrick Doherty, State of New York, Office of the State Comptroller
Sarah Nelson; Louise Rice; Tamara Davis; John Silva; Shana Weiss

EXHIBIT A

Contact: Brad Burns
brad.burns@att.com
(214) 757-3253

AT&T UPDATE ON GOVERNMENT SURVEILLANCE POSITION

Plans to publish semi-annual transparency report

DALLAS, December 20, 2013 – AT&T Inc. (NYSE: T) today provided an update on its position on the government surveillance discussion taking place as well as steps the company plans to take to provide more transparency into government requests for customer information.

The following statement should be attributed to Wayne Watts, AT&T Senior Executive Vice President and General Counsel:

The debate about government surveillance programs and striking the right balance between protecting personal privacy and providing national security is a healthy one. It's important that policymakers worldwide get it right so that people can continue to enjoy the benefits of technology and communications with confidence.

When it comes to governmental surveillance and requests for customer information, all companies are compelled to comply with the laws of the country in which they operate. Those laws not only govern what companies must do when they receive lawful government requests, but often limit what companies can say publicly about the requests. But here is what we can say:

- Protecting our customers' information and privacy is paramount. Everywhere we operate, we go to great lengths to make sure our customers' data is safe and secure. And we do so in compliance with the laws of the country where the service is provided.
- When we receive a government request for customer information, whether it's a court order, a subpoena, or other method, we ensure that the request and our response are completely lawful and proper in that country.
- We work hard to make sure that the requests or orders are valid and that our response to them is lawful. We've challenged court orders, subpoenas and other requests from local, state and federal governmental entities – and will continue to do so, if we believe they are unlawful.
- We do not allow any government agency to connect directly to our network to gather, review or retrieve our customers' information.
- We only provide wireless customer location data in response to a court order except in the rare cases in which an emergency compels us to do so. Examples include when law enforcement enlists us to locate a missing child or a kidnapping suspect, and they provide us assurance that a real emergency affecting human life exists.

To further our efforts to be as transparent as possible within the government guidelines in which we operate, like Verizon recently announced, we intend to publish a semi-annual online report that will

provide information on the number of law enforcement requests for customer information that our company receives in the countries in which we do business. AT&T expects to publish the first report, covering information received in 2013, in early 2014.

To the extent permitted by laws and regulations, AT&T's transparency report will include:

- The total number of law enforcement agency requests received from government authorities in criminal cases;
- Information on the number of subpoenas, court orders and warrants;
- The number of customers affected; and
- Details about the legal demands AT&T receives, as well as information about requests for information in emergencies.

Finally, in our view, any disclosures regarding classified information should come from the government, which is in the best position to determine what can be lawfully disclosed and would or would not harm national security.

We believe clear legal frameworks with accountability and oversight are required to strike the right balance between protecting individual privacy and civil liberties, and protecting the national and personal security, a balance we all desire. We take our responsibility to protect our customers' information and privacy very seriously and pledge to continue to do so to the fullest extent possible.

About AT&T

AT&T Inc. (NYSE:T) is a premier communications holding company and one of the most honored companies in the world. Its subsidiaries and affiliates – AT&T operating companies – are the providers of AT&T services in the United States and internationally. With a powerful array of network resources that includes the nation's fastest and most reliable 4G LTE network, AT&T is a leading provider of wireless, Wi-Fi, high speed Internet, voice and cloud-based services. A leader in mobile Internet, AT&T also offers the best wireless coverage worldwide of any U.S. carrier, offering the most wireless phones that work in the most countries. It also offers advanced TV service with the AT&T U-verse® brand. The company's suite of IP-based business communications services is one of the most advanced in the world.

Additional information about AT&T Inc. and the products and services provided by AT&T subsidiaries and affiliates is available at <http://www.att.com/aboutus> or follow our news on Twitter at @ATT, on Facebook at <http://www.facebook.com/att> and YouTube at <http://www.youtube.com/att>.

© 2013 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners.

4G LTE speed claim based on national carriers' average 4G LTE download speeds. Reliability claim based on data transfer completion rates on nationwide 4G LTE networks. 4G LTE availability varies.

###



Wayne A. Wirtz
Associate General Counsel
Legal Department
208 S. Akard, Room 3024
Dallas, Texas 75202
(214) 757-3344
ww0118@att.com

1934 Act/Rule 14a-8

By email: shareholderproposals@sec.gov

December 5, 2013

U.S. Securities and Exchange Commission
Division of Corporation Finance
Office of Chief Counsel
100 F St., NE
Washington, DC 20549

Re: AT&T Inc. – Request to Exclude Shareholder Proposal of the New York State Common Retirement Fund et al.

Ladies and Gentlemen:

AT&T Inc., a Delaware corporation (“AT&T” or the “Company”), intends to exclude from its proxy statement and form of proxy for its 2014 Annual Meeting of Shareholders (collectively, the “2014 Proxy Materials”) a shareholder proposal (the “Proposal”) and statement in support thereof (the “Supporting Statement”) submitted by the New York State Common Retirement Fund and co-filers Sarah Nelson, Louise Rice, Tamara Davis, John Silva, and Shana Weiss (collectively, the “Proponents”). We have concurrently have sent copies of this correspondence to the Proponents.

Rule 14a-8(k) and Staff Legal Bulletin No. 14D (Nov. 7, 2008) (“SLB 14D”) provide that proponents are required to send companies a copy of any correspondence that the proponents elect to submit to the Commission or the staff of the Division of Corporation Finance (the “Staff”). Accordingly, we are taking this opportunity to inform the Proponents that if they elect to submit additional correspondence to the Commission or the Staff with respect to the Proposal, a copy of that correspondence should be furnished concurrently to the undersigned.

THE PROPOSAL

The Proposal is entitled “Report on Government Requests for Consumer Information.” Following several paragraphs of introductory language, the Proposal sets forth the following resolution to be voted on by shareholders at the 2014 Annual Meeting:

“Resolved, shareholders request that the Company publish semi-annual reports, subject to existing laws and regulation, providing metrics and discussion regarding requests for customer information by U.S. and foreign governments, at reasonable cost and omitting proprietary information.”

The Supporting Statement provides that this report “should be prepared with consideration of existing Transparency (or Law Enforcement Request) Reports published by the major internet companies, and where applicable, include such information as (1) how often AT&T has shared information with U.S. or foreign government entities; (2) what type of customer information was shared; (3) the number of customers affected; (4) type of government requests; and (5) discussion of efforts by the company to protect customer privacy rights.”

The Proposal and Supporting Statement call for such a report because “The Wall Street Journal has reported that AT&T has provided millions of U.S. customers’ call records to the U.S. National Security Agency (NSA). ‘US Collects Vast Data Trove,’ June 7, 2013”; “Controversy over U.S. government surveillance programs reportedly involving AT&T has spurred massive global press coverage, hearings in the U.S. Congress and the European legislature, and widespread calls for reform”; and “The Wall Street Journal has reported that AT&T’s plans to expand its mobile network in Europe, including anticipated acquisitions, could face ‘unexpected hurdles’ due to its cooperation with NSA consumer information requests. ‘NSA Fallout Hurts AT&T’s Ambitions in Europe,’ October 30, 2013.” And “[y]et, the Company has not disclosed to customers and investors any information regarding the extent and nature of requests for customer data made on the Company by government agencies.”

A copy of the Proposal and the Supporting Statement are attached to this letter as Exhibit A. The related correspondence with the Proponents is attached to this letter as Exhibit B.

ARGUMENT

The Proposal Relates to Ordinary Business Matters and May Be Excluded Pursuant to Exchange Act Rule 14a-8(i)(7)

Rule 14a-8(i)(7) permits a company to omit a shareholder proposal from its proxy materials if the proposal deals with a matter relating to the company’s “ordinary business operations.” The purpose of the ordinary business exclusion is “to confine the resolution of ordinary business problems to management and the board of directors, since it is impracticable for shareholders to decide how to solve such problems at an annual shareholders meeting,”¹ and two considerations underlie this exclusion. The first relates to the subject matter of the proposal: “[c]ertain tasks are so fundamental to management’s ability to run a company on a day-to-day basis that they could not, as a practical matter, be subject to direct shareholder oversight.”² The second consideration relates to the “degree to which the proposal seeks to ‘micro-manage’ the

¹ Release No. 34-40018 (May 21, 1998) (the “1998 Release”).

² Id.

company by probing too deeply into matters of a complex nature upon which shareholders, as a group, would not be in a position to make an informed judgment.”³

In applying Rule 14a-8(i)(7) to proposals requesting companies to prepare reports on specific aspects of their business, the Staff has determined that it will consider whether the subject matter of the report involves a matter of ordinary business. If it does, the proposal can be excluded even if it requests only the preparation of the report and not the taking of any action with respect to such ordinary business matter.⁴

Protecting Customer Privacy Is a Management Function.

The Proposal and Supporting Statement ask AT&T to publish reports “providing metrics and discussion regarding requests for customer information by U.S. and foreign governments,” including “discussion of efforts by the company to protect customer privacy rights.” The development and implementation of policies and procedures for the protection of customer information, including the circumstances under which that information may or must be lawfully disclosed, is a core management function and an integral part of AT&T’s day-to-day business operations. The level of privacy provided by AT&T to its customers is fundamental to its service offerings and its ability to attract and retain customers. AT&T has over 100 million customers in over 100 countries. Management is in the best position to determine what policies and procedures are necessary to protect customer privacy, to ensure compliance with applicable legal and regulatory requirements in the states and countries in which we operate, and to apprise AT&T’s customers of the steps that are taken to protect their privacy. To that end, among other things, AT&T has adopted a Privacy Policy,⁵ appointed a Chief Privacy Officer and trained relevant employees on compliance with Company policies and procedures. AT&T’s Code of Business Conduct – which is disseminated to AT&T’s customers – provides that:

- **“We guard the privacy of our customers’ communications.** We protect the privacy of our customers’ communications. Not only do our customers demand this, but the law requires it. Consistent with this principle, although we comply with government requests for customer communications, we do so only to the extent required by law. Maintaining the confidentiality of communications is, and always has been, a crucial part of our business.
- **“We protect the information about our customers that they entrust to us.** AT&T possesses sensitive, detailed information about our customers, who rely on AT&T to safeguard that information. Laws and regulations tell us how to treat such data. Any inappropriate use of confidential customer information violates our customers’ trust and may also violate a law or regulation. Preserving our customers’ trust by safeguarding their private data is essential to our reputation.”⁶

³ Id.

⁴ Release No. 34-20091 (Aug. 16, 1983).

⁵ See AT&T Privacy Policy (available at <http://www.att.com/gen/privacy-policy?pid=2506>).

⁶ See AT&T Code of Business Conduct (available at: http://www.att.com/Common/about_us/downloads/att_code_of_business_conduct.pdf).

In requesting “metrics” as well as “discussion” about government requests for customer information, the Proposal impermissibly seeks to subject AT&T’s customer relations’ policies and practices to shareholder oversight and is therefore excludable under Rule 14a-8(i)(7).

The Staff has long recognized that the protection of customer privacy is a core management function, not subject to shareholder oversight, and has accordingly allowed companies to exclude proposals requesting reports on issues related to customer privacy. For example, in the telecommunications context alone, in *AT&T Inc.* (Feb. 7, 2008), a shareholder proposal requested that AT&T’s Board of Directors prepare a report that discusses “the policy issues that pertain to disclosing customer records and the content of customer communications to federal and state agencies without a warrant, as well as the effect of such disclosure on the privacy rights of customers.” The proposal also emphasized the importance of these issues in light of customers’ right of privacy. The Staff permitted AT&T to exclude the proposal on the ground that it related to “AT&T’s ordinary business operations (i.e., procedures for protecting customer information).” In *Verizon Communications, Inc.* (Feb. 22, 2007), a shareholder proposal requested that the company prepare a report describing “the overarching technological, legal and ethical policy issues surrounding the disclosure of customer records and communications content” to government and non-government agencies. The proposal also emphasized the importance of these issues in terms of customers’ freedom of expression. The Staff allowed Verizon to exclude the proposal from its proxy materials on the ground that it related to “Verizon’s ordinary business operations (i.e., procedures for protecting customer information).”

The Staff has also reached the same conclusion in other business contexts. For example, in *AT&T Inc.* (Jan. 26, 2009), a shareholder proposal requested that AT&T’s Board of Directors prepare a report “examining the effects of the company’s Internet network management practices in the context of the significant public policy concerns regarding the public’s expectations of privacy and freedom of expression on the Internet,” such as the “social and political effects of collecting and selling personal information to third-parties....” The Staff permitted exclusion on the basis that the proposal related to “AT&T’s ordinary business operations (i.e., procedures for protecting user information).” In *Bank of America Corp.* (Feb. 21, 2006), a shareholder proposal requested that Bank of America’s Board of Directors prepare a report on the bank’s policies and procedures for ensuring the confidentiality of customer information, citing several instances of theft of customer information and breaches of cybersecurity. The Staff permitted exclusion on the basis that the proposal related to “Bank of America’s ordinary business operations (i.e., procedures for protecting customer information).”

The Proposal Relates to Ongoing Litigation Involving the Company.

The Proposal may also be omitted under Rule 14a-8(i)(7) because it improperly interferes with the Company’s legal strategy and the discovery process in pending proceedings that allege unlawful acts by AT&T in relation to the alleged provision of customer information to the National Security Agency (“NSA”).

AT&T has been [we only have one known suit at this time – we have not yet been served]a defendant in multiple pending lawsuits that generally allege that AT&T has violated

customer privacy rights by providing information and assistance to government entities without proper legal authority, including allegedly providing information to the NSA. For example, in *Klayman v. Obama*, 1:13-cv-00881-RJL (D.D.C., *complaint filed* June 12, 2013), plaintiffs allege that, “On information and belief, Defendants, providers of remote computing service and electronic communication services to the public, knowingly or intentionally divulged records or other information pertaining to Plaintiffs and Class members to a governmental entity in violation of 18 U.S.C. §2702(a)(3).” Compl. at ¶ 111. In their prayer for relief, plaintiffs demand “a full disclosure and a complete accounting of what each Defendant and government agencies as a whole have done and allowed the DOJ and NSA to do.” Compl. at ¶ 117.

Thus, the Proposal makes similar allegations and calls for the same information requested by the plaintiffs in *Klayman v. Obama* in their prayer for relief – thereby essentially circumventing appropriate restrictions on the discovery process (as well as the judicial process) – and can therefore be excluded from AT&T’s 2014 Proxy Materials as improperly interfering with AT&T’s litigation strategy and intruding upon management’s appropriate discretion to conduct the Company’s litigation as its business judgment dictates in the ordinary course of its day-to-day business operations. In effect, the Proposal would have the Company facilitating discovery by the plaintiffs in *Klayman v. Obama* at the same time the Company is challenging the plaintiffs’ legal positions or claims.

The Staff has previously acknowledged that a shareholder proposal is properly excludable under the “ordinary business” exception when the subject matter of the proposal is the same as or similar to that which is at the heart of litigation in which a company is then involved. See, e.g., *Chevron Corp.* (Mar. 19, 2013) (concurring with the exclusion of a proposal under Rule 14a-8(i)(7) because “the company is presently involved in litigation relating to the subject matter of the proposal” and noting that “[p]roposals that would affect the conduct of ongoing litigation to which the company is a party are generally excludable under rule 14a-8(i)(7)”; and *Merck & Co., Inc.* (Mar. 21, 2012) (concurring with the exclusion under Rule 14a-8(i)(7) of a proposal requesting that the company “file criminal charges against and prosecute all individuals, whose actions or inactions resulted in Merck’s guilty plea,” where the Staff noted that the proposal related to the “conduct of ongoing litigation to which the company is a party”).

This result is also consistent with the Staff’s longstanding position that a company’s decision to institute or defend itself against legal actions and its decisions on how it will conduct those legal actions are matters relating to its ordinary business operations and within the exclusive prerogative of management. See, e.g., *R. J. Reynolds Tobacco Holdings, Inc.* (Feb. 6, 2004) (proposal requiring the company to stop using the terms “light,” “ultralight” and “mild” until shareholders could be assured through independent research that such brands reduce the risk of smoking-related diseases was excluded as ordinary business because it interfered with the litigation strategy of a class-action lawsuit on similar matters involving the company); *NetCurrents, Inc.* (May 8, 2001) (proposal requiring the company to bring an action against certain persons was excluded as ordinary business operations because it related to litigation strategy); and *Exxon Mobil Corp.* (Mar. 21, 2000) (proposal requesting immediate payment of settlements associated with the Exxon Valdez oil spill was excluded because it related to litigation strategy and related decisions).

Overseeing Legal Compliance is a Management Function.

The Proposal can also be properly excluded under Rule 14a-8(i)(7) because it relates to the Company's conduct of its legal compliance program. As stated in AT&T's Privacy Policy, "there are occasions when we provide Personal Information to other companies or other entities, such as government agencies, credit bureaus and collection agencies, without your consent. Some examples include sharing to: Comply with court orders, subpoenas, lawful discovery requests and other legal or regulatory requirements...." The Proposal's request for a report "providing metrics and discussion regarding requests for customer information by U.S. and foreign governments" relates to the Company's compliance with the legal process, which falls squarely within the confines of the Company's ordinary business. "Requests for customer information" would include, among other things, the hundreds of thousands of requests for customer information that AT&T receives each year in the ordinary course of its day-to-day operations from law enforcement agencies and courts throughout the world, such as in the form of subpoenas issued in connection with official criminal investigations, court orders and search warrants issued under the Federal Rules of Criminal Procedure or equivalent state warrant procedures upon a showing of probable cause. Many of these requests are fulfilled in real time as AT&T responds to fire and police emergencies as they occur. To handle these requests, AT&T employs over 130 processors in multiple locations to handle this volume.

The Staff has consistently recognized a company's compliance with law as a matter of ordinary business and proposals relating to a company's legal compliance program as infringing on management's core function of overseeing business practices. For example, in *The AES Corp.* (Jan. 9, 2007), a shareholder proposal sought the creation of a board oversight committee to monitor company compliance with federal, state and local laws. The company argued that compliance with law was so fundamental to management's ability to run the company – particularly since it operated in a heavily regulated industry sector (energy), in which the understanding of and compliance with applicable national, provincial and municipal regulations was critical to its ability to generate, distribute and sell power in any country – that it could not, as a practical matter, be subject to direct shareholder oversight. The Staff concurred with the exclusion of the proposal, noting that the proposal related to "ordinary business operations (i.e., general conduct of a legal compliance program)." See also *Halliburton Company* (Mar. 10, 2006) (proposal requesting a report addressing the potential impact of certain violations and investigations on the company's reputation and stock value and how the company intended to prevent further violations could be excluded as relating to the ordinary business of conducting a legal compliance program).

The Proposal Does Not Focus on a Significant Policy Issue.

The Commission has stated that "proposals relating to such [ordinary business] matters but focusing on sufficiently significant social policy issues (e.g., significant discrimination matters) generally would not be considered to be excludable because the proposals would transcend the day-to-day business matter and raise policy matters so significant that it would be appropriate for a shareholder vote."⁷

⁷ 1998 Release.

We recognize that claims made by former NSA contractor Edward Snowden to The Guardian and The Washington Post in June of this year about the NSA's alleged surveillance activities have generated recent media coverage. These articles have reported that the NSA sought and obtained an order from the Foreign Intelligence Surveillance Court ("FISC") that required Verizon to disclose certain information relating to telephone calls in the U.S. The articles suggest that other FISC orders may require similar disclosures by other communications carriers. Under the Foreign Surveillance Intelligence Act, carriers are prohibited from publicly disclosing FISC orders or the actions that carriers take to comply with the orders.

In the ensuing public debate, no one has seriously disputed that carriers are under an obligation to comply with court orders, so the focus of the media reports has been on the appropriateness of the underlying government surveillance policies and on the government's data collection practices. Thus, the debate in the press and before Congress has focused on proposals to reform the government's practices and the governing legal requirements, not on the disclosure practices of communications carriers with respect either to routine law enforcement requests or alleged court orders that mandate that they provide assistance to the government and that they not disclose that assistance.

Hence, the issue of carrier disclosure practices regarding the NSA's alleged surveillance data collection practices and the "requests for customer data made on the Company by government agencies" more generally has not been raised to the level of "consistent topic of widespread public debate,"⁸ *i.e.*, "sustained public debate over the last several years"⁹ – which are the Staff's characterizations of the standard that must be met in order for a policy to be deemed to be a "significant policy" for purposes of avoiding exclusion under Rule 14a-8(i)(7).¹⁰ In addition, this issue has not been seasoned by the test of time. It is telling that all of the news articles cited in the Proposal were published after June 2013, and that five of the six Internet companies referenced in the Proposal as publishing Transparency or Law Enforcement Request Reports published their first such report in 2012 or 2013.

Regardless Of Whether The Proposal Touches Upon Significant Policy Issues, The Entire Proposal Is Excludable Because It Also Addresses Ordinary Business Matters.

Even if the Staff were to conclude that the issue of carrier disclosure practices regarding the NSA's alleged surveillance data collection practices and the "requests for customer data made on the Company by government agencies" more generally constitutes a significant policy

⁸ See *AT&T* (Feb. 2, 2011) ("We further note that although net neutrality appears to be an important business matter for AT&T and the topic of net neutrality has recently attracted increasing levels of public attention, we do not believe that net neutrality has emerged as a consistent topic of widespread public debate such that it would be a significant policy issue for purposes of rule 14a-8(i)(7).") (emphasis added).

⁹ See *AT&T* (Feb. 10, 2012) ("In view of the sustained public debate over the last several years concerning net neutrality and the Internet and the increasing recognition that the issue raises significant policy considerations, we do not believe that AT&T may omit the proposal from its proxy materials in reliance on rule 14a-8(i)(7).") (emphasis added).

¹⁰ The Commission has directed the Staff to "use the most well-reasoned and consistent standards possible, given the inherent complexity of the task." 1998 Release.

for purposes of Rule 14a-8(i)(7), the mere fact that a proposal touches upon a significant policy issue is not alone sufficient to avoid the application of Rule 14a-8(i)(7) when the proposal also addresses ordinary business matters. *See Intel Corp.* (Mar. 18, 1999) (“There appears to be some basis for your view that Intel may exclude the proposal under rule 14a-8(i)(7), as relating, *in part*, to Intel’s ordinary business operations . . .” (emphasis added)); *General Electric Co.* (Feb. 10, 2000) (concurring in the exclusion of a proposal relating to the discontinuation of an accounting method and use of funds related to an executive compensation program in reliance on Rule 14a-8(i)(7) as dealing with both the significant policy issue of senior executive compensation and the ordinary business matter of choice of accounting method); *Wal-Mart Stores, Inc.* (Mar. 15, 1999) (concurring in the exclusion of a proposal requesting a report on Wal-Mart’s actions to ensure it does not purchase from suppliers who manufacture items using forced labor, convict labor, child labor or who fail to comply with laws protecting employees’ rights in reliance on Rule 14a-8(i)(7) because “paragraph 3 of the description of matters to be included in the report relates to ordinary business operations”).

Here, the “Resolved” paragraph of the Proposal – which constitutes the directive that AT&T’s Board of Directors would be asked to act on if it is adopted by AT&T’s shareholders at the 2014 Annual Meeting – is stated in its entirety as follows:

“Resolved, shareholders request that the Company publish semi-annual reports, subject to existing laws and regulation, providing metrics and discussion regarding requests for customer information by U.S. and foreign governments, at reasonable cost and omitting proprietary information.”

This directive covers all requests for customer information by U.S. and foreign governments and would include, among other things, the many requests for customer information that AT&T receives from federal, state and local law enforcement agencies and courts throughout the world, such as in the form of subpoenas issued in connection with official criminal investigations, court orders and search warrants issued under the Federal Rules of Criminal Procedure or equivalent state warrant procedures upon a showing of probable cause. The Supporting Statement makes the broad scope of the “Resolved” paragraph clear by referencing, as examples for AT&T to follow in preparing these reports, the “existing Transparency (or Law Enforcement Request) Reports published by the major internet companies.” The introductory paragraphs before the “Resolved” paragraph name “Google, Microsoft, Twitter, LinkedIn, Facebook and Yahoo!” as examples of major Internet companies.

We have reviewed these companies’ Transparency or Law Enforcement Request Reports:

- Google (<http://www.google.com/transparencyreport/userdatarequests/countries/?t=table>);
- Microsoft (<https://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/>);
- Twitter (<https://blog.twitter.com/2012/twitter-transparency-report>);
- LinkedIn (http://help.linkedin.com/app/answers/detail/a_id/41878);

- Facebook (<https://www.facebook.com/safety/groups/law/guidelines/>, https://www.facebook.com/about/government_requests); and
- Yahoo! (<http://info.yahoo.com/transparency-report/us/>)

All of them include information about requests for information received by law enforcement agencies outside of the national security-related context.

Indeed, because any information about assistance that AT&T has, or has not, provided to the government in connection with the government's foreign intelligence surveillance activities would almost certainly be classified information that AT&T could not legally disclose, the report sought in the Proposal, "subject to existing laws and regulation," would necessarily be limited to the Company's routine law enforcement compliance in the ordinary course of business. (In fact, all six Internet companies referenced in the Proposal state that they are not allowed to publicly disclose any such information in their Transparency or Law Enforcement Request Reports.) Therefore, because the Proposal is over-broad, it is excludable under Rule 14a-8(i)(7) as relating, in large part, to the ordinary business matter of compliance with legal process, even if the Staff were to conclude that it also addresses a significant policy.

CONCLUSION

Based upon the foregoing analysis, we respectfully request that the Staff concur that it will take no action if the Company excludes the Proposal from its 2014 Proxy Materials.

We would be happy to provide you with any additional information and answer any questions that you may have regarding this subject. Correspondence regarding this letter should be sent to me at ww0118@att.com. If I can be of any further assistance in this matter, please do not hesitate to contact me at (214) 757-3344.

Sincerely,



Encl.: Exhibit A
Exhibit B

cc: Patrick Doherty, State of New York, Office of the State Comptroller (via email: pdoherty@osc.state.ny.us)
Sarah Nelson (via email: john@harringtoninvestments.com)
Louise Rice (via email: jkron@trilliuminvest.com)
Tamara Davis (via email: Natasha@arjuna-capital.com)
John Silva (via email: Natasha@arjuna-capital.com)
Shana Weiss (via email: Natasha@arjuna-capital.com)

EXHIBIT A

Report on Government Requests for Consumer Information

Whereas,

Customer trust is critical for any business, but especially for major Internet and telecommunications companies that routinely gather massive amounts of personal data concerning and affecting the lives of hundreds of millions of people in the U.S. and around the world.

The Wall Street Journal has reported that AT&T has provided millions of U.S. customers' call records to the U.S. National Security Agency (NSA). "US Collects Vast Data Trove," June 7, 2013.

AT&T acknowledges in its corporate code of conduct that privacy is critical to the success of its business. Yet, the Company has not disclosed to customers and investors any information regarding the extent and nature of requests for customer data made on the Company by government agencies.

Controversy over U.S. government surveillance programs reportedly involving AT&T has spurred massive global press coverage, hearings in the U.S. Congress and the European legislature, and widespread calls for reform. Brazilian President Dilma Rousseff called the NSA surveillance program "a breach of international law." U.S. Senator Ron Wyden said, "I have to believe the civil liberties of millions of American have been violated."

Responding to growing public concern over these issues, major Internet companies such as Google, Microsoft, Twitter, LinkedIn, Facebook and Yahoo!, have published "Transparency Reports", disclosing information on government data requests. Google and Microsoft have also filed in court seeking authorization to disclose further information to the public concerning these requests. AT&T has not done so.

The Wall Street Journal has reported that AT&T's plans to expand its mobile network in Europe, including anticipated acquisitions, could face "unexpected hurdles" due to its co-operation with NSA consumer information requests. "NSA Fallout Hurts AT&T's Ambitions in Europe," October 30, 2013.

Transparency in this regard is essential if individuals and businesses are to make informed decisions regarding their personal data. Privacy is a fundamental tenet of democracy and free expression. While AT&T must comply with its legal obligations, failure to persuade customers of a genuine and long-term commitment to privacy rights could present AT&T with serious financial, legal and reputational risks.

Resolved, shareholders request that the Company publish semi-annual reports, subject to existing laws and regulation, providing metrics and discussion regarding requests for customer information by U.S. and foreign governments, at reasonable cost and omitting proprietary information.

Supporting Statement: In preparing these reports, the Company may, at its discretion, omit information on routine requests provided under individualized warrants. The reports should be prepared with consideration of existing Transparency (or Law Enforcement Request) Reports published by the major internet companies, and where applicable, include such information as (1) how often AT&T has shared information with U.S. or foreign government entities; (2) what type of customer information was shared; (3) the number of customers affected; (4) type of government requests; and (5) discussion of efforts by the company to protect customer privacy rights.

[rev. Nov 11]

EXHIBIT B

THOMAS P. DINAPOLI
STATE COMPTROLLER



STATE OF NEW YORK
OFFICE OF THE STATE COMPTROLLER

PENSION INVESTMENTS
& CASH MANAGEMENT
633 Third Avenue-31st Floor
New York, NY 10017
Tel: (212) 681-4489
Fax: (212) 681-4468

November 7, 2013

Ms. Ann E. Meuleman
Senior Vice President and
Secretary
AT&T Corporation
208 S. Akard Street, Suite 3241
Dallas, Texas 75202

Dear Ms. Meuleman:

The Comptroller of the State of New York, Thomas P. DiNapoli, is the sole Trustee of the New York State Common Retirement Fund (the "Fund") and the administrative head of the New York State and Local Employees' Retirement System and the New York State Police and Fire Retirement System. The Comptroller has authorized me to inform AT&T Corporation of his intention to offer the enclosed shareholder proposal for consideration of stockholders at the next annual meeting.

I submit the enclosed proposal to you in accordance with rule 14a-8 of the Securities Exchange Act of 1934 and ask that it be included in your proxy statement.

A letter from J.P. Morgan Chase, the Fund's custodial bank, verifying the Fund's ownership, continually for over a year, of AT&T Corporation shares, will follow. The Fund intends to continue to hold at least \$2,000 worth of these securities through the date of the annual meeting.

We would be happy to discuss this initiative with you. Should the board decide to endorse its provisions as company policy, we will ask that the proposal be withdrawn from consideration at the annual meeting. Please feel free to contact me at (212) 681-4823 and/or pdoherty@osc.state.ny.us, should you have any further questions on this matter.

Very truly yours,

A handwritten signature in dark ink, appearing to read "Patrick Doherty", written over a horizontal line.

Patrick Doherty
pd:jm
Enclosures

Report on Government Requests for Consumer Information

Whereas,

Customer trust is critical for any business, but especially for major Internet and telecommunications companies that routinely gather massive amounts of personal data concerning and affecting the lives of hundreds of millions of people in the U.S. and around the world.

The Wall Street Journal has reported that AT&T has provided millions of U.S. customers' call records to the U.S. National Security Agency (NSA). "US Collects Vast Data Trove," June 7, 2013.

AT&T acknowledges in its corporate code of conduct that privacy is critical to the success of its business. Yet, the Company has not disclosed to customers and investors any information regarding the extent and nature of requests for customer data made on the Company by government agencies.

Controversy over U.S. government surveillance programs reportedly involving AT&T has spurred massive global press coverage, hearings in the U.S. Congress and the European legislature, and widespread calls for reform. Brazilian President Dilma Rousseff called the NSA surveillance program "a breach of international law." U.S. Senator Ron Wyden said, "I have to believe the civil liberties of millions of American have been violated."

Responding to growing public concern over these issues, major Internet companies such as Google, Microsoft, Twitter, LinkedIn, Facebook and Yahoo!, have published "Transparency Reports", disclosing information on government data requests. Google and Microsoft have also filed in court seeking authorization to disclose further information to the public concerning these requests. AT&T has not done so.

The Wall Street Journal has reported that AT&T's plans to expand its mobile network in Europe, including anticipated acquisitions, could face "unexpected hurdles" due to its co-operation with NSA consumer information requests. "NSA Fallout Hurts AT&T's Ambitions in Europe," October 30, 2013.

Transparency in this regard is essential if individuals and businesses are to make informed decisions regarding their personal data. Privacy is a fundamental tenet of democracy and free expression. While AT&T must comply with its legal obligations, failure to persuade customers of a genuine and long-term commitment to privacy rights could present AT&T with serious financial, legal and reputational risks.

Resolved, That the Company publish semi-annual reports, subject to existing laws and regulation, providing metrics and discussion regarding requests for customer information by U.S. and foreign governments, at reasonable cost and omitting proprietary information.

Supporting Statement: In preparing these reports, the Company may, at its discretion, omit information on routine requests provided under individualized warrants. The reports should be prepared with consideration of existing Transparency (or Law Enforcement Request) Reports published by the major internet companies, and where applicable, include such information as (1) how often AT&T has shared information with U.S. or foreign government entities; (2) what type of customer information was shared; (3) the number of customers affected; (4) type of government requests; and (5) discussion of efforts by the company to protect the privacy of customer data.

RECEIVED

NOV 11 2013

CORPORATE
SECRETARY'S OFFICE

SANFORD J. LEWIS, ATTORNEY

November 11, 2013

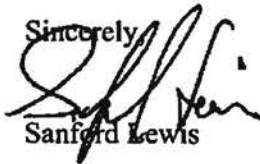
Ms. Ann E. Meuleman
Senior Vice President and
Secretary
AT & T Corporation
208 S. Akard Street, Suite 3241
Dallas, Texas 75202

Dear Ms. Meuleman:

I am writing on behalf of Thomas P. DiNapoli, the sole Trustee of the New York State Common Retirement Fund (the "Fund") and the administrative head of the New York State and Local Employees' Retirement System and the New York State Police and Fire Retirement System. The Comptroller has authorized me to submit the enclosed revised shareholder proposal for the 2014 annual meeting. You should have previously received the enclosed letter dated Nov. 7, 2013 from Patrick Doherty regarding the proposal. The enclosed revised proposal replaces the proposal submitted by Mr. Doherty, and his enclosed letter in all other aspects stands as written with regard to this revised version.

Please call me at (413) 549-7333 with respect to any questions in connection with this matter.

Sincerely,



Sanford Lewis

Report on Government Requests for Consumer Information

Whereas,

Customer trust is critical for any business, but especially for major Internet and telecommunications companies that routinely gather massive amounts of personal data concerning and affecting the lives of hundreds of millions of people in the U.S. and around the world.

The Wall Street Journal has reported that AT&T has provided millions of U.S. customers' call records to the U.S. National Security Agency (NSA). "US Collects Vast Data Trove," June 7, 2013.

AT&T acknowledges in its corporate code of conduct that privacy is critical to the success of its business. Yet, the Company has not disclosed to customers and investors any information regarding the extent and nature of requests for customer data made on the Company by government agencies.

Controversy over U.S. government surveillance programs reportedly involving AT&T has spurred massive global press coverage, hearings in the U.S. Congress and the European legislature, and widespread calls for reform. Brazilian President Dilma Rousseff called the NSA surveillance program "a breach of international law." U.S. Senator Ron Wyden said, "I have to believe the civil liberties of millions of American have been violated."

Responding to growing public concern over these issues, major Internet companies such as Google, Microsoft, Twitter, LinkedIn, Facebook and Yahoo!, have published "Transparency Reports", disclosing information on government data requests. Google and Microsoft have also filed in court seeking authorization to disclose further information to the public concerning these requests. AT&T has not done so.

The Wall Street Journal has reported that AT&T's plans to expand its mobile network in Europe, including anticipated acquisitions, could face "unexpected hurdles" due to its co-operation with NSA consumer information requests. "NSA Fallout Hurts AT&T's Ambitions in Europe," October 30, 2013.

Transparency in this regard is essential if individuals and businesses are to make informed decisions regarding their personal data. Privacy is a fundamental tenet of democracy and free expression. While AT&T must comply with its legal obligations, failure to persuade customers of a genuine and long-term commitment to privacy rights could present AT&T with serious financial, legal and reputational risks.

Resolved, shareholders request that the Company publish semi-annual reports, subject to existing laws and regulation, providing metrics and discussion regarding requests for customer information by U.S. and foreign governments, at reasonable cost and omitting proprietary information.

Supporting Statement: In preparing these reports, the Company may, at its discretion, omit information on routine requests provided under individualized warrants. The reports should be prepared with consideration of existing Transparency (or Law Enforcement Request) Reports published by the major internet companies, and where applicable, include such information as (1) how often AT&T has shared information with U.S. or foreign government entities; (2) what type of customer information was shared; (3) the number of customers affected; (4) type of government requests; and (5) discussion of efforts by the company to protect customer privacy rights.

[rev. Nov 11]

Senior Vice President and Secretary
AT&T Inc.
208 S. Akard St. Suite 3241
Dallas, TX 75202

RECEIVED

NOV 08 2013

**CORPORATE
SECRETARY'S OFFICE**

Dear Secretary:

Trillium Asset Management LLC ("Trillium") is an investment firm based in Boston specializing in socially responsible asset management. We currently manage approximately \$1.3 billion for institutional and individual clients.

Trillium hereby submits the enclosed shareholder proposal with AT&T, Inc. on behalf of Louise Rice for inclusion in the 2014 proxy statement and in accordance with Rule 14a-8 of the General Rules and Regulations of the Securities and Exchange Act of 1934 (17 C.F.R. § 240.14a-8). Per Rule 14a-8, Louise Rice holds more than \$2,000 of AT&T Inc. common stock, acquired more than one year prior to today's date and held continuously for that time. As evidenced in the attached letter, Louise Rice will remain invested in this position continuously through the date of the 2014 annual meeting. We will forward verification of the position separately. We will send a representative to the stockholders' meeting to move the shareholder proposal as required by the SEC rules.

We are co-filers for this proposal in which the lead filer is the Office of the New York State Comptroller.

We would welcome discussion with AT&T Inc. about the contents of our proposal.

Please direct any communications to me at (503) 592-0864, or via email at jkron@trilliuminvest.com.

We would appreciate receiving a confirmation of receipt of this letter via email.

Sincerely,



Jonas Kron
Senior Vice President, Director of Shareholder Advocacy
Trillium Asset Management, LLC

Cc: Randall L. Stephenson, Chairman and Chief Executive Officer

Enclosures

November 15, 2013

Senior Vice President and Secretary
AT&T Inc.
208 S. Akard St., Suite 3241
Dallas, TX 75202

Dear Secretary:

In accordance with the SEC Rules, please find the attached authorization letter from Louise Rice as well as the custodial letter from Charles Schwab Advisor Services documenting that she holds sufficient company shares to file a proposal under rule 14a-8.

Please contact me if you have any questions at (503) 592-0864; Trillium Asset Management LLC, 711 Atlantic Ave., Boston, MA 02111; or via email at jkron@trilliuminvest.com.

Sincerely,



Jonas Kron
Senior Vice President, Director of Shareholder Advocacy
Trillium Asset Management, LLC

Cc: Randall L. Stephenson, Chairman and Chief Executive Officer

Enclosures

BOSTON

711 Atlantic Avenue
Boston, Massachusetts 02111-2429
T: 617-424-6655 F: 617-422-5120
800-548-5684

DURHAM

383 West Main Street, Second Floor
Custom Sports Center, 27701-3245
T: 319-688-1264 F: 319-688-1451
800-853-1311

SAN FRANCISCO BAY

100 Lakeside Landing Circle, Suite 405
Larkspur, California 94904-1741
T: 415-925-0107 F: 415-925-0109
800-933-4806

Jonas Kron
Vice President, Director of Shareholder Advocacy
Trillium Asset Management, LLC
711 Atlantic Avenue
Boston, MA 02111

Fax: 617 482 6179

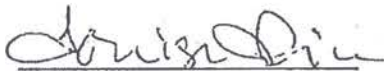
Dear Mr. Kron:

I hereby authorize Trillium Asset Management LLC to file a shareholder proposal on my behalf at AT&T, Inc. (T).

I am the beneficial owner of more than \$2,000 worth of common stock in AT&T that I have held continuously for more than one year. I intend to hold the aforementioned shares of stock through the date of the company's annual meeting in 2014.

I specifically give Trillium Asset Management, LLC full authority to deal, on my behalf, with any and all aspects of the aforementioned shareholder proposal. I understand that my name may appear on the corporation's proxy statement as the filer of the aforementioned proposal.

Sincerely,



Louise Rice
c/o Trillium Asset Management LLC
711 Atlantic Avenue, Boston, MA 02111

10/9/13
Date

charles SCHWAB
ADVISOR SERVICES

1958 Summit Park Dr, Orlando, FL 32810

November 11, 2013

Re: Louise B. Rice**~~FOIA~~ & OMB Memorandum M-07-16 ***

This letter is to confirm that Charles Schwab & Co. holds as custodian for the above account 429 shares of AT&T Inc. common stock. These 429 shares have been held in this account continuously for one year prior to November 7, 2013.

These shares are held at Depository Trust Company under the nominee name of Charles Schwab & Company.

This letter serves as confirmation that the shares are held by Charles Schwab & Co, Inc.

Sincerely,



JM Brodie
Director



TRILLIUM ASSET MANAGEMENT®

Delivering Sustainable Investments Since 1982SM

November 11, 2013

Senior Vice President and Secretary
AT&T Inc.
208 S. Akard St. Suite 3241
Dallas, TX 75202

Dear Secretary:

Trillium Asset Management, LLC ("Trillium") recently submitted a shareholder proposal, as a co-filer to lead filer the Office of the New York State Comptroller, with the Company on behalf of our client. See attached letter.

Enclosed please find a revised proposal that was submitted by The Office of the New York State Comptroller earlier today. This proposal is filed consistent with Staff Legal Bulletin No. 14F issued on October 18, 2011 regarding revised proposals. Furthermore, The Office of the New York State Comptroller represented in its letter that it was acting on behalf of Trillium, which in turn is action on behalf of its client Louise Rouse. This letter is being submitted out of an abundance of caution and to confirm the submission of the revised proposal on behalf of our client Louise Rice.

Trillium hereby submits the enclosed shareholder proposal with AT&T, Inc. on behalf of Louise Rice for inclusion in the 2014 proxy statement and in accordance with Rule 14a-8 of the General Rules and Regulations of the Securities and Exchange Act of 1934 (17 C.F.R. § 240.14a-8). Per Rule 14a-8, Louise Rice holds more than \$2,000 of AT&T Inc. common stock, acquired more than one year prior to today's date and held continuously for that time. As evidenced in the attached letter, Louise Rice will remain invested in this position continuously through the date of the 2014 annual meeting. We will forward verification of the position separately. We will send a representative to the stockholders' meeting to move the shareholder proposal as required by the SEC rules.

This is a co-filing of the proposal in which the lead filer is the Office of the New York State Comptroller.

We would appreciate receiving a confirmation of receipt of this letter via email.

Sincerely,

Jonas Kron
Senior Vice President, Director of Shareholder Advocacy
Trillium Asset Management, LLC

Cc: Randall L. Stephenson, Chairman and Chief Executive Officer

Enclosures

SANFORD J. LEWIS, ATTORNEY

November 11, 2013

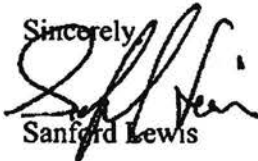
Ms. Ann E. Meuleman
Senior Vice President and
Secretary
AT & T Corporation
208 S. Akard Street, Suite 3241
Dallas, Texas 75202

Dear Ms. Meuleman:

I am writing on behalf of the co-filer Louise Rice, for whom a shareholder proposal for the 2014 shareholder meeting of AT&T Inc. was filed on her behalf by Trillium Asset Management. Trillium, on behalf of their client, has authorized and requested that I submit the enclosed revision to that proposal on her behalf as a co-filer.

Please call me at (413) 549-7333 with respect to any questions in connection with this matter.

Sincerely,



Sanford Lewis



November 7, 2013

AT&T Corp
Senior Vice President and Secretary
208 S. Akard Street, Suite 3241
Dallas, TX 75202

RECEIVED

NOV 08 2013

**CORPORATE
SECRETARY'S OFFICE**

RE: Shareholder Proposal

Dear Secretary,

I hereby submit on behalf of our client, Sarah Nelson, the enclosed shareholder proposal for the 2014 shareholder meeting of AT&T Inc. Sarah has authorized and requested that I submit this proposal on her behalf as a co-filer, and out of honor and respect for the work of the Northern California ACLU.

As a cofiler, Sarah designates as lead filer, Thomas P. DiNapoli, Comptroller of the State of New York, who has filed this proposal on behalf of the New York State Common Retirement Fund, as my spokesperson for any dialogue regarding this proposal, and as having the authority to withdraw the proposal.

This proposal is submitted for inclusion in the 2014 proxy statement, in accordance with rule 14a-8 of the General Rules and Regulations of the Securities and Exchange Act of 1934 (17 C.F.R. § 240.14a-8). Harrington Investments submits this proposal on behalf of our client, who is the beneficial owner, per rule 14a-8, of more than \$2,000 worth of AT&T common stock acquired more than one year prior to today's date. Our client will remain invested in this position through the date of the company's 2014 annual meeting. I have enclosed a copy of Proof of Ownership from Charles Schwab & Company. We will send a representative to the stockholders' meeting to move the proposal as required by the Securities and Exchange Commission rules.

If you desire to discuss the substance of the proposal, please contact me at (707) 252-6166.

Thank you.

Sincerely,

John C. Harrington
President

Report on Government Requests for Consumer Information

Whereas,

Customer trust is critical for any business, but especially for major Internet and telecommunications companies that routinely gather massive amounts of personal data concerning and affecting the lives of hundreds of millions of people in the U.S. and around the world.

The Wall Street Journal has reported that AT&T has provided millions of U.S. customers' call records to the U.S. National Security Agency (NSA). "US Collects Vast Data Trove," June 7, 2013.

AT&T acknowledges in its corporate code of conduct that privacy is critical to the success of its business. Yet, the Company has not disclosed to customers and investors any information regarding the extent and nature of requests for customer data made on the Company by government agencies.

Controversy over U.S. government surveillance programs reportedly involving AT&T has spurred massive global press coverage, hearings in the U.S. Congress and the European legislature, and widespread calls for reform. Brazilian President Dilma Rousseff called the NSA surveillance program "a breach of international law." U.S. Senator Ron Wyden said, "I have to believe the civil liberties of millions of Americans have been violated."

Responding to growing public concern over these issues, major Internet companies such as Google, Microsoft, Twitter, LinkedIn, Facebook and Yahoo!, have published "Transparency Reports", disclosing information on government data requests. Google and Microsoft have also filed in court seeking authorization to disclose further information to the public concerning these requests. AT&T has not done so.

The Wall Street Journal has reported that AT&T's plans to expand its mobile network in Europe, including anticipated acquisitions, could face "unexpected hurdles" due to its co-operation with NSA consumer information requests. "NSA Fallout Hurts AT&T's Ambitions in Europe," October 30, 2013.

Transparency in this regard is essential if individuals and businesses are to make informed decisions regarding their personal data. Privacy is a fundamental tenet of democracy and free expression. While AT&T must comply with its legal obligations, failure to persuade customers of a genuine and long-term commitment to privacy rights could present AT&T with serious financial, legal and reputational risks.

Resolved, That the Company publish semi-annual reports, subject to existing laws and regulation, providing metrics and discussion regarding requests for customer information by U.S. and foreign governments, at reasonable cost and omitting proprietary information.

Supporting Statement: In preparing these reports, the Company may, at its discretion, omit information on routine requests provided under individualized warrants. The reports should be prepared with consideration of existing Transparency (or Law Enforcement Request) Reports published by the major internet companies, and where applicable, include such information as (1) how often AT&T has shared information with U.S. or foreign government entities; (2) what type of customer information was shared; (3) the number of customers affected; (4) type of government requests; and (5) discussion of efforts by the company to protect the privacy of customer data.

charles SCHWAB
ADVISOR SERVICES

PO Box 52013, Phoenix, AZ 85072-2013

November 7, 2013

AT&T Corp
Senior Vice President and Secretary
208 S. Akard Street, Suite 3241
Dallas, Texas 75202

RE: **Account** SMA & OMB Memorandum M-07-16 ***
Sarah B. Nelson Living Trust

Dear Secretary:

This letter is to verify that Sarah B. Nelson has continuously held at least \$2000 in market value of AT&T stock for at least one year prior to November 7, 2013.

Should additional information be needed, please feel free to contact me directly at 877-393-1951 between the hours of 11:30am and 8:00pm EST.

Sincerely,



Patricia Stewart
Advisor Services
Charles Schwab & Co. Inc.

SANFORD J. LEWIS, ATTORNEY

November 11, 2013

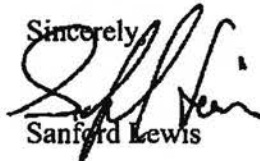
Ms. Ann E. Meuleman
Senior Vice President and
Secretary
AT & T Corporation
208 S. Akard Street, Suite 3241
Dallas, Texas 75202

Dear Ms. Meuleman:

I am writing on behalf of the cofiler Sarah Nelson, who previously cofiled a shareholder proposal for the 2014 shareholder meeting of AT&T Inc. Sarah has authorized and requested that I submit the enclosed revision to that proposal on her behalf as a co-filer, and out of honor and respect for the work of the Northern California ACLU.

Please call me at (413) 549-7333 with respect to any questions in connection with this matter.

Sincerely,



Sanford Lewis

November 8th, 2013

Natasha Lamb

Director of Equity Research & Shareholder Engagement

Arjuna Capital/Baldwin Brothers Inc.

353 West Main Street

Durham, NC 27701

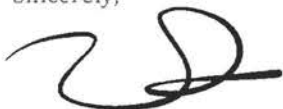
Dear Ms. Lamb,

I hereby authorize Arjuna Capital/Baldwin Brothers Inc. to file a shareholder proposal on my behalf at AT&T regarding a Report on Government Requests for Customer Information.

I am the beneficial owner of more than \$2,000 worth of common stock in AT&T that I have held continuously for more than one year. I intend to hold the aforementioned shares of stock through the date of the company's annual meeting in 2014.

I specifically give Arjuna Capital/Baldwin Brothers Inc. full authority to deal, on my behalf, with any and all aspects of the aforementioned shareholder proposal. I understand that my name may appear on the corporation's proxy statement as the filer of the aforementioned proposal.

Sincerely,



Tamara Davis

c/o Arjuna Capital/Baldwin Brothers Inc.

353 West Main Street

Durham, NC 27701

charles SCHWAB
ADVISOR SERVICES

1958 Summit Park Dr, Orlando, FL 32810

November 8th, 2013

Ann E. Meuleman
Senior Vice President and Secretary of AT&T
208 S. Akard Street, Suite 3241
Dallas, Texas 75202

Dear Ms. Meuleman or WHOM IT MAY CONCERN:

Re: Tamra Davis / SMA & OMB Memorandum M-07-16 ***

This letter is to confirm that Charles Schwab & Co is the record holder for the beneficial owners of the account of above, which Arjuna Capital, the sustainable wealth management platform of Baldwin Brothers Inc. manages and which holds in the account MB Memorandum 125 shares of common stock in AT&T.*.

As of November 8th, Tamra Davis held, and has held continuously for at least one year, 125 shares of AT&T stock.

This letter serves as confirmation that the account holder listed above is the beneficial owner of the above referenced stock.

Sincerely,



*DATE: insert the date that the stock position was received by the custodian
07/06/2007



November 8th, 2013

Ann E. Meuleman
Senior Vice President and Secretary of AT&T
208 S. Akard Street, Suite 3241
Dallas, Texas 75202

Dear Ms. Meuleman:

Arjuna Capital is the sustainable wealth management platform of Baldwin Brothers, Inc., an investment firm based in Marion, MA.

I am hereby authorized to notify you of our intention to co-file the enclosed shareholder resolution with AT&T on behalf of our clients Tamara Davis and John Silva and Shana Weiss. Arjuna Capital/Baldwin Brothers Inc. submits this shareholder proposal for inclusion in the 2014 proxy statement, in accordance with Rule 14a-8 of the General Rules and Regulations of the Securities and Exchange Act of 1934 (17 C.F.R. § 240.14a-8). Per Rule 14a-8, Tamara Davis and John Silva and Shana Weiss hold more than \$2,000 of AT&T common stock, acquired more than one year prior to today's date and held continuously for that time. Our clients will remain invested in this position continuously through the date of the 2014 annual meeting. Enclosed please find verification of the position and a letter from Tamara Davis and John Silva and Shana Weiss authorizing Arjuna Capital/Baldwin Brothers Inc. to undertake this filing on their behalf. We will send a representative to the stockholders' meeting to move the shareholder proposal as required by the SEC rules.

We would welcome discussion with AT&T about the contents of our proposal.

Please direct any written communications to me at the address below or to natasha@arjuna-capital.com. Please also confirm receipt of this letter via email.

Sincerely,

Natasha Lamb
Director of Equity Research & Shareholder Engagement
Arjuna Capital/Baldwin Brothers Inc.
204 Spring Street □ Marion, MA 02738

Cc: Randall L. Stephenson, Chairman and Chief Executive Officer

Enclosures

November 4 2013

Natasha Lamb
Director of Equity Research & Shareholder Engagement
Arjuna Capital
353 West Main Street
Durham, NC 27701

Dear Ms. Lamb,

I hereby authorize Arjuna Capital to file a shareholder proposal on my behalf at AT&T regarding a Report on Government Requests for Customer Information.

I am the beneficial owner of more than \$2,000 worth of common stock in AT&T that I have held continuously for more than one year. I intend to hold the aforementioned shares of stock through the date of the company's annual meeting in 2014.

I specifically give Arjuna Capital full authority to deal, on my behalf, with any and all aspects of the aforementioned shareholder proposal. I understand that my name may appear on the corporation's proxy statement as the filer of the aforementioned proposal.

Sincerely,


John Silva

Shana Weiss

c/o Arjuna Capital
353 West Main Street
Durham, NC 27701

November 8, 2013

Natasha Lamb
Director of Equity Research & Shareholder Engagement
Arjuna Capital
353 West Main Street
Durham, NC 27701

Dear Ms. Lamb,

I hereby authorize Arjuna Capital to file a shareholder proposal on my behalf at AT&T regarding a Report on Government Requests for Customer Information.

I am the beneficial owner of more than \$2,000 worth of common stock in AT&T that I have held continuously for more than one year. I intend to hold the aforementioned shares of stock through the date of the company's annual meeting in 2014.

I specifically give Arjuna Capital full authority to deal, on my behalf, with any and all aspects of the aforementioned shareholder proposal. I understand that my name may appear on the corporation's proxy statement as the filer of the aforementioned proposal.

Sincerely,

John Silva

A handwritten signature in black ink, appearing to read "Shana Weiss", written over a horizontal line.

Shana Weiss

c/o Arjuna Capital
353 West Main Street
Durham, NC 27701

charles SCHWAB
ADVISOR SERVICES

1958 Summit Park Dr, Orlando, FL 32810

November 8th, 2013

Ann E. Meuleman
Senior Vice President and Secretary of AT&T
208 S. Akard Street, Suite 3241
Dallas, Texas 75202

Dear Ms. Meuleman or WHOM IT MAY CONCERN:

Re: John Silva and Shana Weiss & OMB Memorandum M-07-16 ***

This letter is to confirm that Charles Schwab & Co. is the record holder for the beneficial owners of the account of above, which Arjuna Capital, the sustainable wealth management platform of Baldwin Brothers Inc. manages and which holds in the account 150 shares of common stock in AT&T*.

As of November 8th, John Silva and Shana Weiss held, and has held continuously for at least one year, 150 shares of AT&T stock.

This letter serves as confirmation that the account holder listed above is the beneficial owner of the above referenced stock.

Sincerely,



*DATE: insert the date that the stock position was received by the custodian
9/17/2007