

From: Mogil, Joshua (ODAG)
Subject: Updated Privacy Remarks
To: Brown Lee, Erika (ODAG)
Cc: Bruck, Andrew J. (ODAG)
Sent: October 17, 2016 4:22 PM (UTC-04:00)
Attached: Tuesday- Privacy Forum Remarks.docx
Any updates to these remarks, Erika? Thank you very much!

Best,
Josh

From: Brown Lee, Erika (ODAG)
Subject: Re: OPCL Draft of DAG Remarks for Privacy Forum
To: Winn, Peter A. (OPCL)
Cc: Lane Scott, Kristi Z (OPCL)
Sent: October 18, 2016 1:57 PM (UTC-04:00)

Were you able to update the doc?

Erika Brown Lee
Chief Privacy and Civil Liberties Officer
United States Department of Justice
[950 Pennsylvania Avenue, NW](#)
[Washington, D.C. 20530](#)
(b) (6)

On Oct 18, 2016, at 3:22 PM, Brown Lee, Erika (ODAG) <(b) (6)> wrote:

Hi Peter, Kristi - I've edited the text below. Kindly re-insert into the document and review for grammar and content and then resend to me and I'll send to ODAG.

Thank you!
Erika

Erika Brown Lee
Chief Privacy and Civil Liberties Officer
Office of the Deputy Attorney General
United States Department of Justice
950 Pennsylvania Avenue, NW
Washington, D.C. 20530
Tel: (b) (6)
(b) (6)


On Oct 18, 2016, at 2:45 PM, Winn, Peter A. (OPCL) <(b) (6)> wrote:

DOJ PRIVACY FORUM
DOJ Conference Center, Room 7411, RFK Main Justice Building
Tuesday, October 25, 2016, at 10:30 a.m. POC: Erika Brown Lee, ODAG/CPCLO, (b) (6)
(b) (6)

SUGGESTED REMARKS FOR
DEPUTY ATTORNEY GENERAL SALLY YATES

(b) (5)

(b) (5)

A large rectangular area of text is completely redacted with a solid black fill.

(b) (5)

A large rectangular area of text is completely redacted with a solid black fill.

(b) (5)

A large rectangular area of text is completely redacted with a solid black fill.

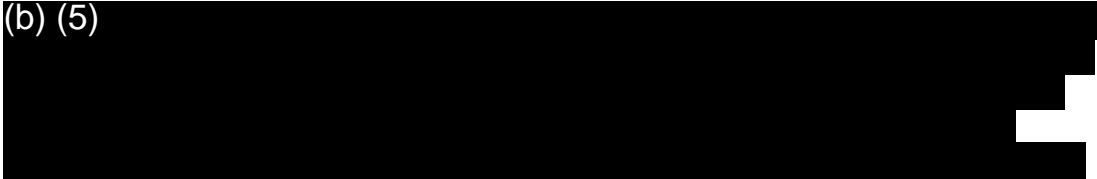
(b) (5)

A large rectangular area of text is completely redacted with a solid black fill.

(b) (5)

A large rectangular area of text is completely redacted with a solid black fill.

(b) (5)

A large rectangular area of text is completely redacted with a solid black fill.

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

From: Brown Lee, Erika (ODAG)
Sent: Tuesday, October 18, 2016 9:18 AM
To: Winn, Peter A. (OPCL)

Cc: Lane Scott, Kristi Z (OPCL)

Subject: Re: OPCL Draft of DAG Remarks for Privacy Forum

Ok great - I'm on my way back to my room now. Please call my cell in 10?

Erika Brown Lee

Chief Privacy and Civil Liberties Officer

United States Department of Justice

[950 Pennsylvania Avenue, NW](#)

[Washington, D.C. 20530](#)

(b) (6)

On Oct 18, 2016, at 2:15 PM, Winn, Peter A. (OPCL) <(b) (6)> wrote:

I'm available now and can take your edits.

Peter

Peter A. Winn

Director, Office of Privacy and Civil Liberties

United States Department of Justice

National Place Building, Suite 1000

1331 Pennsylvania Avenue, NW

Washington DC 20530

Office (b) (6)

Cell (b) (6)

Fax (202) 307-0693

(b) (6)

From: Brown Lee, Erika (ODAG)

Sent: Tuesday, October 18, 2016 9:15 AM

To: Winn, Peter A. (OPCL)

Cc: Lane Scott, Kristi Z (OPCL)

Subject: Re: OPCL Draft of DAG Remarks for Privacy Forum

Hi Peter Kristi - any chance you're available for a quick call now about the remarks? I'm having trouble editing from here, but ODAG needs them as soon as possible.

Thanks,

Erika

Erika Brown Lee

Chief Privacy and Civil Liberties Officer

United States Department of Justice

[950 Pennsylvania Avenue, NW](#)

[Washington, D.C. 20530](#)

(b) (6)

On Oct 14, 2016, at 8:54 PM, Winn, Peter A. (OPCL)

<(b) (6)> wrote:

Hi Erika,

Here is the OPCL draft of the DAG's remarks, for your review.

Peter

Peter A. Winn
Director, Office of Privacy and Civil Liberties
United States Department of Justice
National Place Building, Suite 1000
1331 Pennsylvania Avenue, NW
Washington DC 20530
Office (b) (6)
Cell (b) (6)
Fax (202) 307-0693
(b) (6)

<DAG Privacy Forum Remarks OPCL DRAFT.docx>

From: Winn, Peter A. (OPCL)
Subject: RE: OPCL Draft of DAG Remarks for Privacy Forum
To: Brown Lee, Erika (ODAG)
Cc: Lane Scott, Kristi Z (OPCL)
Sent: October 18, 2016 2:36 PM (UTC-04:00)
Attached: DAG Privacy Forum Remarks Final.docx

Hi Erika,

Sorry for the delay. When I got back from the Privacy Council, I got waylaid by a couple of issues that had a short fuse.

The new version looks fine. I just fixed a few minor typos, and then cut and pasted the remarks into the attached reformatted document.

Hopefully, you should be able to just forward on this version of the document.

Peter

Peter A. Winn
Director, Office of Privacy and Civil Liberties
United States Department of Justice
National Place Building, Suite 1000
1331 Pennsylvania Avenue, NW
Washington DC 20530
Office (b) (6)
Cell (b) (6)
Fax (202) 307-0693
(b) (6)

From: Winn, Peter A. (OPCL)
Subject: RE: OPCL Draft of DAG Remarks for Privacy Forum
To: Brown Lee, Erika (ODAG)
Sent: October 18, 2016 3:28 PM (UTC-04:00)
Attached: DAG Privacy Forum Remarks Final.docx

Here is the new version with the edits.

Peter

From: Brown Lee, Erika (ODAG)
Sent: Tuesday, October 18, 2016 3:09 PM
To: Winn, Peter A. (OPCL)
Subject: Re: OPCL Draft of DAG Remarks for Privacy Forum

Spotted one edit. Can you give me a quick call?

Erika Brown Lee
Chief Privacy and Civil Liberties Officer

United States Department of Justice

[950 Pennsylvania Avenue, NW](#)

[Washington, D.C. 20530](#)

(b) (6)

On Oct 18, 2016, at 7:43 PM, Winn, Peter A. (OPCL) <(b) (6)> wrote:

Hi Erika,

I just noticed that the earlier version had the wrong time. It was also missing page numbers.

Please review this version.

Peter

Peter A. Winn
Director, Office of Privacy and Civil Liberties
United States Department of Justice
National Place Building, Suite 1000
1331 Pennsylvania Avenue, NW
Washington DC 20530
Office (b) (6)
Cell (b) (6)
Fax (202) 307-0693
(b) (6)

<DAG Privacy Forum Remarks Final.docx>

From: Brown Lee, Erika (ODAG)
Subject: Draft of DAG Remarks for Privacy Forum
To: Mogil, Joshua (ODAG); Bruck, Andrew J. (ODAG)
Sent: October 18, 2016 3:43 PM (UTC-04:00)
Attached: DAG Privacy Forum Remarks Final.docx, ATT00001.htm

Josh, Andrew - attached for consideration is a draft of the DAG's remarks for the Privacy Forum. Please let me know if you have any questions.

Best,
Erika

Erika Brown Lee
Chief Privacy and Civil Liberties Officer
United States Department of Justice
[950 Pennsylvania Avenue, NW](#)
[Washington, D.C. 20530](#)
(b) (6)

From: Brown Lee, Erika (ODAG)
Subject: Draft of DAG Remarks for Privacy Forum
To: Mogil, Joshua (ODAG); Bruck, Andrew J. (ODAG)
Bcc: Brown Lee, Erika (ODAG)
Sent: October 18, 2016 3:43 PM (UTC-04:00)
Attached: DAG Privacy Forum Remarks Final.docx, ATT00001.htm

Josh, Andrew - attached for consideration is a draft of the DAG's remarks for the Privacy Forum. Please let me know if you have any questions.

Best,
Erika

Erika Brown Lee
Chief Privacy and Civil Liberties Officer

United States Department of Justice

[950 Pennsylvania Avenue, NW](#)

[Washington, D.C. 20530](#)

(b) (6)

From: Bruck, Andrew J. (ODAG)
Subject: Draft -- Privacy Forum TPs
To: Axelrod, Matthew (ODAG); Childs, Heather G. (ODAG)
Sent: October 21, 2016 1:39 AM (UTC-04:00)
Attached: Draft - DAG Privacy Forum TPs.docx, Draft - DAG Privacy Forum Remarks.docx

Erika sent draft remarks for the DAG's appearance at the DOJ Privacy Forum on Tuesday. I actually think these should be TPs instead – it's closed press, fed gov't employees only, with only brief remarks from the DAG.

I tried distilling the remarks to TPs, although there wasn't much content to work with. I've also attached Erika's unedited remarks.

From: Bruck, Andrew J. (ODAG)
Subject: Privacy Forum TPs -- Tues 10/25 @ 10:30 am
To: Mogil, Joshua (ODAG)
Cc: Axelrod, Matthew (ODAG); Childs, Heather G. (ODAG)
Sent: October 21, 2016 12:32 PM (UTC-04:00)
Attached: Draft - DAG Privacy Forum TPs.docx

Attached. Since this is an internal event, I converted Erika's speech into TPs.

<<Draft - DAG Privacy Forum TPs.docx>>

From: Bruck, Andrew J. (ODAG)
Subject: Privacy Forum TPs -- Tues 10/25 @ 10:30 am
To: Mogil, Joshua (ODAG)
Cc: Axelrod, Matthew (ODAG); Childs, Heather G. (ODAG)
Sent: October 21, 2016 12:32 PM (UTC-04:00)
Attached: Draft - DAG Privacy Forum TPs.docx

Attached. Since this is an internal event, I converted Erika's speech into TPs.

From: Mogil, Joshua (ODAG)
Subject: FW: Privacy Forum TPs -- Tues 10/25 @ 10:30 am
To: Yates, Sally (ODAG)
Sent: October 21, 2016 12:37 PM (UTC-04:00)
Attached: Draft - DAG Privacy Forum TPs.docx
[Privacy Forum points. I'll also print hard copy for your weekend book.](#)

From: Bruck, Andrew J. (ODAG)
Sent: Friday, October 21, 2016 12:32 PM
To: Mogil, Joshua (ODAG)
Cc: Axelrod, Matthew (ODAG); Childs, Heather G. (ODAG)
Subject: Privacy Forum TPs -- Tues 10/25 @ 10:30 am

Attached. Since this is an internal event, I converted Erika's speech into TPs.

From: Young, Brian A. (OPCL)
Subject: RE: Privacy Forum - Surveillance Technologies Panel - RESCHEDULED for October 25
To: Douglass, Sean (OLP)
Sent: October 21, 2016 1:20 PM (UTC-04:00)
Hi Sean.

Did you ever send me a bio for yourself? If not, could you please do that?

Thanks,
Brian

Brian A. Young
Senior Counsel
Office of Privacy and Civil Liberties (OPCL)
U.S. Department of Justice
(b) (6) (office)
(b) (6) (mobile)
(202) 307-0693 (fax)
SECRET: (b) (6)
TS: (b) (6)

NOTICE: This email (including any attachments) is intended for the use of the individual or entity to which it is addressed. It may contain information that is privileged, confidential, or otherwise protected by applicable law. If you are not the intended recipient (or the recipient's agent), you are hereby notified that any dissemination, distribution, copying, or use of this email or its contents is strictly prohibited. If you received this email in error, please notify the sender immediately and destroy all copies.

From: Douglass, Sean (OLP)
Sent: Tuesday, September 27, 2016 4:24 PM
To: Young, Brian A. (OPCL)
Cc: Winn, Peter A. (OPCL); Lane Scott, Kristi Z (OPCL); Quinn, Maura F. (DEA); Bordley, Ed (USMS); O'Shea, Michael
Subject: RE: Privacy Forum - Surveillance Technologies Panel - RESCHEDULED for October 25

Duplicative Information - See Document ID 0.7.12327.58000



From: Lane Scott, Kristi Z (OPCL)
Subject: DOJ Privacy Forum Final Agenda
To: Andrews, Carla (OPCL)
Cc: Winn, Peter A. (OPCL)
Sent: October 21, 2016 3:40 PM (UTC-04:00)
Attached: DOJ Privacy Forum 2016.pdf

Please use this version to send out to the attendees. I made one correction to the agenda.



United States Department of Justice

Privacy Forum

Presented by the Chief Privacy and Civil Liberties Officer and the Office of Privacy and Civil Liberties

October 25, 2016

RFK Main, Attorney General's Conference Room 7411

9:00 AM to 3:30 PM

9:00 - 9:15 AM	Welcome <ul style="list-style-type: none">Erika Brown Lee, Chief Privacy and Civil Liberties Officer
9:15 – 10:15 AM	Cyber Threat Information Sharing (<i>Moderated by Andrew Proia</i>) <ul style="list-style-type: none">Leonard Bailey, DOJ/CCIPS, Special Counsel for National SecurityDianna Carr, DHS/NPPD, Deputy DirectorJames Burd, DHS/NPPD, Senior Privacy Analyst(b)(6), (7)(C) per FBI, FBI/OGC, Assistant General Counsel
10:15 – 10:25 AM	Break
10:30 – 10:45 AM	Remarks by Deputy Attorney General, Sally Q. Yates
10:45 – 11:30 AM	Use of Social Media: Opportunities and Challenges (<i>Moderated by Kristi Lane Scott</i>) <ul style="list-style-type: none">(b)(6), (7)(C) per FBI, FBI/OGC, Privacy and Civil Liberties, Unit ChiefDavid Lindner, DHS, Office of Privacy, Privacy AnalystPeggy O'Neil, Open Source Enterprise, Legal CounselAshley McGowan, DOJ/OPA, Digital Engagement Manager
11:30 – 12:30 PM	Lunch (<i>On your own</i>)
12:40 – 1:00 PM	Remarks on the Federal Privacy Council and Other Privacy Community Updates <ul style="list-style-type: none">Marc Groman, OMB, Senior Advisor for Privacy
1:00 – 1:50 PM	Surveillance Technologies: UAS and Cell Site Simulators (<i>Moderated by Brian Young</i>) <ul style="list-style-type: none">Mark Greene, DOJ, Office of Justice PolicySean Douglass, DOJ, Office of Legal PolicyEd Bordley, USMS, Associate General Counsel(b)(6), (7)(C), (7)(F) per DEA, DEA, Office of General Counsel
1:50 – 2:00 PM	Break
2:00 - 2:50 PM	Insider Threat (<i>Moderated by Peter Winn</i>) <ul style="list-style-type: none">(b)(6), (7)(C) per FBI, FBI, Insider Threat, Unit ChiefArthur Gary, DOJ/JMD, General CounselCarrie Staugler, DOJ/JMD, Program Manager for Insider Threat(b)(3), (b)(6) per ODNI, ODNI, Deputy Privacy and Civil Liberties Officer
2:50 – 3:30 PM	Information Security Breaches and Incident Response (<i>Moderated Hannah Mayer/Khaliah Barnes</i>) <ul style="list-style-type: none">Erika Brown Lee, DOJ, Chief Privacy and Civil Liberties OfficerJoo Chung, DOD, Director, Directorate for Oversight and Compliance OfficeJoseph Klimavicz, DOJ, Chief Information Officer
3:30 PM	Closing Remarks , Peter Winn, Director, OPCL

From: Exton, Jasmine (OPCL)
Subject: Privacy Forum Slides
To: Lane Scott, Kristi Z (OPCL)
Sent: October 21, 2016 4:50 PM (UTC-04:00)
Attached: Privacy Forum Slides.pptx

Hi Kristi,

Please find attached the Privacy Forum Slides. Let me know if there are any changes you would like for me to make or anything else to include.

Best,

Jasmine

From: Lane Scott, Kristi Z (OPCL)
Subject: Privacy Forum Slides.pptx
To: Andrews, Carla (OPCL)
Cc: Greer, Christopher M. (JMD)
Sent: October 24, 2016 3:14 PM (UTC-04:00)
Attached: Privacy Forum Slides.pptx



U.S. Department of Justice Privacy Forum

Presented by the Chief Privacy and Civil Liberties Officer
and the Office of Privacy and Civil Liberties

Tuesday, October 25, 2016

RFK Main, Attorney General's Conference Room 7411

9:00 AM to 3:30 PM

Welcome

9:00-9:15 AM

Erika Brown Lee, Chief Privacy and Civil Liberties Officer

Panel 1:

Cyber Threat Information

Sharing

9:15-10:15 AM

This panel will focus on how the Department and its partners share and use cyber threat information, the privacy rules that govern cyber threat information sharing, and the impact these rules have on the government's information sharing initiatives.

Break

10:15-10:25 AM

Remarks

10:30-10:45 AM

Deputy Attorney General, Sally Q. Yates

Panel 2:

Use of Social Media: Opportunities and Challenges

10:45-11:30 AM

This panel will examine the federal government's proactive use of social media to enhance transparency, as well as the Constitutional concerns associated with the operational use of social media in the law enforcement and national security contexts.

Lunch

11:30-12:30 PM

Key Note Remarks

Office of Management and Budget

12:40-1:00 PM

Marc Groman, OMB, Senior Advisor for Privacy

Panel 3:

Surveillance Technologies: UAS and Cell Site Simulators

1:00-1:50 PM

This panel will discuss the privacy and civil liberties aspects of these policies, how these policies are being implemented by Department components, and how DOJ is working under these policies with state and local agencies.

Break

1:50-2:00 PM

Panel 4: Insider Threat

2:00-2:50 PM

This panel will examine issues arising from the implementation of insider threat programs. Such programs are designed to identify threats posed by trusted insiders who may intentionally or negligently do harm to the government's policies, programs and information systems. The implementation of such programs present both operational challenges as well as challenges in connection with balancing vigilant oversight with risks to the privacy and civil liberties of the government employees who are monitored.

Panel 5:

Information Security Breaches and Incident Response

2:50-3:30 PM

This panel will discuss federal government initiatives to help mitigate the risks of information security incidents and breaches. This panel brings together diverse perspectives on how privacy professionals can more robustly protect personally identifiable information.

Closing Remarks

3:30 PM

Peter Winn, Director, OPCL

From: Winn, Peter A. (OPCL)
Subject: Revised Remarks for CPCLO
To: Brown Lee, Erika (ODAG)
Cc: Lane Scott, Kristi Z (OPCL)
Sent: October 24, 2016 5:49 PM (UTC-04:00)
Attached: CPCLO Privacy Forum Remarks 10 24.docx

Erika,

Here is a draft of some revised remarks for you tomorrow.

Peter

Peter A. Winn
Director, Office of Privacy and Civil Liberties
United States Department of Justice
National Place Building, Suite 1000
1331 Pennsylvania Avenue, NW
Washington DC 20530
Office (b) (6)
Cell (b) (6)
Fax (202) 307-0693
(b) (6)

From: Lane Scott, Kristi Z (OPCL)
Subject: Fwd: Privacy Forum Slides.pptx
To: Brown Lee, Erika (ODAG); Winn, Peter A. (OPCL)
Sent: October 24, 2016 8:37 PM (UTC-04:00)
Attached: Privacy Forum Slides with DOD slides.pptx, ATT00001.htm

For your reference.

Begin forwarded message:

From: "Barnes, Khalia N. (OPCL)" <(b) (6)>
To: "Andrews, Carla (OPCL)" <(b) (6)>
Cc: "Mayer, Hannah J. (OPCL)" <(b) (6)>, "Lane Scott, Kristi Z (OPCL)" <(b) (6)>
Subject: RE: Privacy Forum Slides.pptx

Hi Carla,

Please find attached a slide deck with DOD slides.

Thank you,
Khaliah

From: Lane Scott, Kristi Z (OPCL)
Sent: Monday, October 24, 2016 11:41 AM
To: Andrews, Carla (OPCL)
Cc: Mayer, Hannah J. (OPCL); Barnes, Khalia N. (OPCL)
Subject: Privacy Forum Slides.pptx

Carla,

You can use these slides for the dry run. Khaliah and Hannah are going to incorporate Joo's slides into the final presentation.

Thanks,

Kristi



U.S. Department of Justice Privacy Forum

Presented by the Chief Privacy and Civil Liberties Officer
and the Office of Privacy and Civil Liberties

Tuesday, October 25, 2016
RFK Main, Attorney General's Conference Room 7411
9:00 AM to 3:30 PM

Welcome

9:00-9:15 AM

Erika Brown Lee, Chief Privacy and Civil Liberties Officer

Panel 1:

Cyber Threat Information

Sharing

9:15-10:15 AM

This panel will focus on how the Department and its partners share and use cyber threat information, the privacy rules that govern cyber threat information sharing, and the impact these rules have on the government's information sharing initiatives.

Break

10:15-10:25 AM

Remarks

10:30-10:45 AM

Deputy Attorney General, Sally Q. Yates

Panel 2:

Use of Social Media: Opportunities and Challenges

10:45-11:30 AM

This panel will examine the federal government's proactive use of social media to enhance transparency, as well as the Constitutional concerns associated with the operational use of social media in the law enforcement and national security contexts.

Lunch

11:30-12:30 PM

Key Note Remarks

Office of Management and Budget

12:40-1:00 PM

Marc Groman, OMB, Senior Advisor for Privacy

Panel 3:

Surveillance Technologies: UAS and Cell Site Simulators

1:00-1:50 PM

This panel will discuss the privacy and civil liberties aspects of these policies, how these policies are being implemented by Department components, and how DOJ is working under these policies with state and local agencies.

Break

1:50-2:00 PM

Panel 4: Insider Threat

2:00-2:50 PM

This panel will examine issues arising from the implementation of insider threat programs. Such programs are designed to identify threats posed by trusted insiders who may intentionally or negligently do harm to the government's policies, programs and information systems. The implementation of such programs present both operational challenges as well as challenges in connection with balancing vigilant oversight with risks to the privacy and civil liberties of the government employees who are monitored.

Panel 5:

Information Security Breaches and Incident Response

2:50-3:30 PM

This panel will discuss federal government initiatives to help mitigate the risks of information security incidents and breaches. This panel brings together diverse perspectives on how privacy professionals can more robustly protect personally identifiable information.



DoD Breach Response Procedures

Joo Y. Chung

**Director, Oversight and Compliance
Senior Agency Official for Privacy
Department of Defense**



DoD Breach Procedures

DoD policy: Each Component is required to have policies and procedures in place to address breach incidents

DoD Components are also encouraged to assess each breach on a case by case bases using five factors before determining if notification will be required to affected individuals:

1. How the loss occurred;
2. Nature of the data elements breached and number of individuals affected;
3. Ability and likelihood that information is accessible and useful;
4. Ability of the agency to mitigate the risk of harm; and
5. Evidence and likelihood a breach may lead to harm




Reporting a Breach

- DoD components must report all breaches through a system called CART
- Use the DD2959 form – Breach of PII report to standardize information provided
- Departmental review of all breaches to address systemic concerns such as:
 - Emails with sensitive data sent to personal emails
 - Lap tops without data at rest encryption technology
 - Files sent without encryption --
<https://safe.amrdec.army.mil/safe/>

http://www.doncio.navy.mil/Content/View.aspx?ID=852

File Edit View Favorites Tools Help

Log in EBIS Login version 2.10.23 DCPDS Portal - Login Web Slice Gallery performance myPay Web Site

 DEPARTMENT OF THE NAVY
Chief Information Officer

search

HOME POLICY & GUIDANCE NEWS CONTACT US RSS FEEDS

Trending DADMS/DITPR-DON Cybersecurity Privacy IA BROWSE ALL TOPICS

Print Email

PII Breach Reporting Resources

Published, January 21, 2009

The following breach-related resources are provided to aid in reporting the loss or suspected loss of personally identifiable information (PII).

- [PII Breach Reporting Process \(DON CIO WASHINGTON DC 291652Z FEB 08\)](#)
- [Automated PII Breach Reporting Form \(SECNAV 5211/1\)](#)
- [Automated PII Breach After Action Form \(SECNAV 5211/2\)](#)
- [Sample Breach Notification Letter](#)
- [GSA Awards BPAs for Identity Monitoring, Data Breach Response and Protection Services](#)
- [Use of Best Judgment for Individual PII Breach Notification Determinations](#)
- [Consequences for Failing to Safeguard PII](#)
- [Obtaining Contact Information for Notifications](#)
- [Procedure for Establishing a Call Center](#)
- [Instructions for Using WinZip to Encrypt Files](#)

Related Policy

- [Improving Critical Infrastructure Cybersecurity](#)
- [Processing of Electronic Storage Media for Disposal](#)
- [Reduction of SSN Use Within DoD](#)
- [PKI Interoperability with FVEY Partner Nations on the NIPRNet](#)
- [DON Public Affairs Policy and Regulations](#)
- [View More](#)

Related News

- [DON IT West and East 2017 Conference Registration Now Open](#)
- [Nominations for DON IM/IT Excellence Awards Due Dec. 5](#)

TAGS: Cybersecurity, IDManagement, Privacy

Browser address bar: <https://safe.amrdec.army.mil/safe/Welcome.aspx>

Browser tabs: dtic.mil, U.S. GA..., data at..., AMR..., Depart..., How do..., dpcid.d...

Browser menu: File, Edit, View, Favorites, Tools, Help

Browser toolbar: Log in, EBIS Login version 2.10.23, DCPDS Portal - Login, Web Slice Gallery, performance, myPay Web Site

AMRDEC SAFE Home About Help

SAFE

Safe Access File Exchange

SAFE is designed to provide AMRDEC and its customers an alternative way to send files other than email. SAFE supports file sizes up to 2GB.

[Click here for Getting Started Guide](#)

To begin using SAFE please click on one of the links below.

Welcome to the AMRDEC SAFE Web Application

CAC Users

This option is for CAC users with a computer configured for CAC use. When prompted for a certificate, select the one with "EMAIL" in the name.

[Click Here](#)

Or

Non-CAC Users

For users without a CAC OR if your computer is not configured to read your CAC. Using this option will allow you to access SAFE as a [guest](#).

[Click Here](#)

How Does it Work?

Breach Reporting Procedures

TIMELINE	REPORT TO
Within <u>1 HOUR</u> of breach discovery	United States Computer Emergency Readiness Team (US-CERT) (All cyber related, no paper)
Within <u>24 HOURS</u> of breach discovery	Senior Component Official for Privacy (SCOP)
Within <u>48 HOURS</u> of SCOP being notified	Defense Privacy, Civil Liberties and Transparency Division (DPCLTD)
With substantial risk of harm to individuals, notify affected individuals no later than 10 WORKING DAYS after breach discovery and identities of affected individuals known	

DoD's role in OPM cybersecurity incidents

- DoD has about 85% of the cleared population and was actively involved in providing assistance to OPM after the cybersecurity incidents
- Helped Award Identity Protection contract in Aug 2015 - provides services to individuals impacted by the OPM background investigation breach
- Established a Notification Process
- Established a Verification Center

How is DoD Protecting Information?

- Building a robust layered cyber enterprise
- Ensuring up-to-date policies are in place
- Implementing best privacy practices
 - Identifying HVAs and ensuring privacy assessments are conducted and up-to-date
 - Incorporating privacy controls into cybersecurity risk management framework
 - Reducing collection of unnecessary PII and SSNs by policy

Panel 5:

Information Security Breaches and Incident Response

2:50-3:30 PM

This panel will discuss federal government initiatives to help mitigate the risks of information security incidents and breaches. This panel brings together diverse perspectives on how privacy professionals can more robustly protect personally identifiable information.

Closing Remarks

3:30 PM

Peter Winn, Director, OPCL

From: Erika Brown Lee
Subject: Forum Remarks
To: Brown Lee, Erika (ODAG)
Sent: October 25, 2016 6:31 AM (UTC-04:00)
Attached: CPCLO Privacy Forum Opening Remarks.docx

From: Mogil, Joshua (ODAG)
Subject: RE: DAG Comments at the Privacy Forum
To: Brown Lee, Erika (ODAG)
Cc: Bruck, Andrew J. (ODAG); Iverson, Dena W. (OPA); Childs, Heather G. (ODAG)
Sent: November 3, 2016 10:14 AM (UTC-04:00)
Attached: Privacy Forum.docx

+Team to advise if this is ok. I forget this was in note form and not formal remarks. Sorry, Erika.

It was considered closed press so she wrote them in bullet form, not speech form. She wrote it in her own short form system- leaving words out, etc and adlibbing when she memorized a part she didn't need to include. She also didn't expect these to be public-facing messaging so attaching for review.

-Josh

Joshua L. Mogil
Special Assistant to the Deputy Attorney General
U.S. Department of Justice
D: (b) (6), C: (b) (6)
(b) (6)

From: Brown Lee, Erika (ODAG)
Sent: Wednesday, November 02, 2016 6:06 PM
To: Mogil, Joshua (ODAG) <(b) (6)>
Subject: DAG Comments at the Privacy Forum

Hi Josh – I wanted to follow up on my request for the DAG's comments at the Privacy Forum last week. As I mentioned, people found her words inspirational, and we'd like to include them on OPCL's website, as we did with DAG Cole's comments for the 2014 Forum.

Best regards,
Erika

Erika Brown Lee
Chief Privacy and Civil Liberties Officer
Office of the Deputy Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, D.C. 20530
Tel: (b) (6)
(b) (6)
TS: (b) (6)

From: Mayer, Hannah J. (OPCL)
Subject: Draft Annual Report
To: Winn, Peter A. (OPCL)
Sent: November 18, 2016 10:36 AM (UTC-05:00)
Attached: AnnualPrivacyReport_v.1.docx
Hi Peter,

Please find attached the draft annual report.

Best,

Hannah

Hannah Mayer
Law Clerk
Office of Privacy and Civil Liberties
U.S. Department of Justice
National Place Building, Suite 1000
1331 Pennsylvania Avenue, NW
Washington, DC 20530

(b) (6) (office)

(b) (6) (cell)

202.307.0693 (fax)

(b) (6)

Case No. 14-17339

**IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT**

AMERICAN CIVIL LIBERTIES UNION OF NORTHERN
CALIFORNIA and SAN FRANCISCO BAY GUARDIAN,

PLAINTIFFS- APPELLEES,

v.

UNITED STATES DEPARTMENT OF JUSTICE,

DEFENDANT-APPELLANT.

On Appeal from the United States District Court
for the Northern District of California
No. 3:12-cv-04008-MEJ
The Honorable Maria-Elena James, Magistrate Judge

PLAINTIFFS-APPELLEES' ANSWERING BRIEF

LINDA LYE (SBN 215584)
llye@aclunc.org
MICHAEL T. RISHER (SBN 191627)
mrisher@aclunc.org
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION OF
NORTHERN CALIFORNIA, INC.
39 Drumm Street
San Francisco, CA 94111
Telephone: (415) 621-2493
Facsimile: (415) 255-8437

Attorneys for Plaintiffs-Appellees

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rule of Appellate Procedure 26.1, I certify that Plaintiffs-Appellees American Civil Liberties Union of Northern California and San Francisco Bay Guardian do not have parent corporations and that no publicly held corporation owns 10% or more of any stake or stock in either entity.

DATED: June 22, 2015

By: /s/ Linda Lye
Linda Lye

TABLE OF CONTENTS

INTRODUCTION1

JURISDICTIONAL STATEMENT3

ISSUES PRESENTED.....4

STATEMENT OF FACTS4

 A. The Public Has a Significant Interest in Learning
 about the Government’s Location Tracking Policies
 and Procedures4

 B. The Public Faces Significant Barriers to Obtaining
 Information about the Legal Safeguards Followed
 by the Government7

 C. Plaintiffs Submitted a FOIA Request for Information
 about DOJ’s Location Tracking Policies and Procedures.....9

 D. DOJ Withheld Documents Pursuant to FOIA’s Exemption
 5 and 7(E)11

 E. The Decision Below13

 F. Applications for Location Tracking Orders Filed in
 Court by the U.S. Attorney’s Office are Sealed Indefinitely15

STANDARD OF REVIEW17

SUMMARY OF ARGUMENT17

ARGUMENT20

 I. Exemption 5 Does not Shield from Disclosure a Manual
 for Prosecutors Setting Forth Legal Standards.....20

 A. FOIA Favors Disclosure over Secrecy20

 B. General Legal Protocols for Using Location
 Tracking Technologies Do not Constitute Attorney
 Work Product24

 1. Courts in FOIA Cases Consistently Require
 the Government to Demonstrate a Specific
 Claim to Establish the Work-Product Privilege24

 2. The Specific-Claim Requirement Applies
 Where the Government Acts to Enforce the Law29

 3. The Specific-Claim Test Applies to this
 Case and Compels the Conclusion that the
 USABook is not Work Product33

 4. The USABook Is not Work Product Even
 If the Specific-Claim Requirement Does not Apply34

C. DOJ’s Position on the Legal Prerequisites for Obtaining
Location Tracking Orders Constitutes the Agency’s
Working Law37

II. Disclosure of Legal Standards Used to Engage in Well Known
Location Tracking Techniques Does not Give Rise to
a Risk of Circumvention41

A. Exemption 7(E) Requires the Government to Explain Why
Disclosure of “Details” Risks Circumvention42

B. DOJ Failed to Meet its Burden of Demonstrating a Risk of
Circumvention.....48

C. The Agency Is not Entitled to a Second Chance to
Meet its Burden56

CONCLUSION58

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>American Civil Liberties Union of Northern California v. Dep't of Justice</i> , No. 13-cv-03127-MEJ (N.D. Cal. June 17, 2015), ECF No. 53	36
<i>American Immigration Council v. United States Dep't of Homeland Security</i> , 905 F. Supp. 2d 206 (D.D.C. 2012).....	28, 29
<i>In re Application</i> , 534 F. Supp. 2d 585 (W.D. Pa. 2008).....	<i>passim</i>
<i>Asian Law Caucus v. United States Dep't of Homeland Security</i> , No. 08-00842, 2008 WL 5047839 (N.D. Cal. Nov. 24, 2008).....	47
<i>Assembly of State of California v. United States Dep't of Commerce</i> , 968 F.2d 916 (9th Cir. 1992)	22
<i>Atel Fin. Corp. v. Quaker Coal Co.</i> , 321 F.3d 924 (9th Cir. 2003)	17
<i>Barnard v. Dep't of Homeland Security</i> , 598 F. Supp. 2d 1 (D.D.C. 2009).....	47
<i>Blackwell v. FBI</i> , 646 F.3d 37 (D.C. Cir. 2011).....	45
<i>Bowen v. FDA</i> , 925 F.2d 1225 (9th Cir. 1991)	45, 47, 53
<i>Branch v. FBI</i> , 658 F. Supp. 204 (D.D.C. 1987).....	55
<i>Brunetti v. FBI</i> , 357 F. Supp. 2d 97 (D.D.C. 2004).....	54
<i>Building and Const. Trades Council v. Associated Builders and Contractors of Massachusetts</i> , 507 U.S. 218 (1993).....	32

<i>Church of Scientology of California v. United States Dep’t of Army</i> , 611 F.2d 738 (9th Cir. 1979)	23, 57
<i>Coastal States Gas Corp. v. Dep’t of Energy</i> , 617 F.2d 854 (D.C. Cir. 1980)	<i>passim</i>
<i>Crooker v. Bureau of Alcohol, Tobacco & Firearms</i> , 670 F.2d 1051 (D.C. Cir. 1981)	22
<i>Davin v. United States Dep’t of Justice</i> , 60 F.3d 1043 (3d Cir. 1995)	<i>passim</i>
<i>Delaney, Migdail & Young v. IRS</i> , 826 F.2d 124 (D.C. Cir. 1987)	29, 30, 35
<i>Dep’t of Air Force v. Rose</i> , 425 U.S. 352 (1976)	20, 23, 33
<i>Feshbach v. SEC</i> , 5 F. Supp. 2d 774 (N.D. Cal. 1997)	45
<i>Hale v. United States Dep’t of Justice</i> , 973 F.2d 894 (10th Cir. 1992), <i>cert. granted, vacated and remanded on other grounds</i> , 509 U.S. 918 (1993)	47
<i>Hawkes v. IRS</i> , 507 F.2d 481 (6th Cir. 1974)	48, 52
<i>Hickman v. Taylor</i> , 329 U.S. 495 (1947)	24, 33
<i>Holmgren v. State Farm Mut. Auto. Ins. Co.</i> , 976 F.2d 573 (9th Cir. 1992)	24, 36
<i>Jones v. FBI</i> , 41 F.3d 238 (6th Cir. 1994)	14, 46
<i>Jordan v. United States Dep’t of Justice</i> , 591 F.2d 753 (D.C. Cir. 1978)	<i>passim</i>
<i>Judicial Watch v. United States Dep’t of Homeland Security</i> , 926 F. Supp. 2d 121 (D.D.C. 2013)	28, 29, 32

<i>Kamman v. IRS</i> , 56 F.3d 46 (9th Cir. 1995)	23, 46, 56
<i>Kent Corp. v. NLRB</i> , 530 F.2d 612 (5th Cir. 1976)	27
<i>Maguire v. Mawn</i> , No. 02 Civ. 2164, 2004 WL 1124673 (S.D.N.Y. May 19, 2004)	54
<i>Marbury v. Madison</i> , 1 Cranch 137 (1803)	39
<i>Mead Data Cent., Inc. v. United States Dep't of the Air Force</i> , 566 F.2d 242 (D.C. Cir. 1977)	55
<i>Miller v. United States Dep't of Justice</i> , 562 F. Supp. 2d 82 (D.D.C. 2008)	54
<i>Milner v. Dep't of Navy</i> , 562 U.S. 562 (2011)	22
<i>Minier v. Central Intelligence Agency</i> , 88 F.3d 796 (9th Cir. 1996)	23
<i>Morgan v. United States Dep't of Justice</i> , 923 F.2d 195 (D.C. Cir. 1991)	17
<i>National Ass'n of Criminal Defense Lawyers v. EOUSA</i> , No. 14-269, _F. Supp. 3d _, 2014 WL 7205392 (D.D.C. Dec 18, 2014)	31
<i>National Council of La Raza v. Dep't of Justice</i> , 411 F.3d 350 (2d Cir. 2005)	37
<i>NLRB v. Robbins Tire & Rubber Co.</i> , 437 U.S. 214 (1978)	33
<i>NLRB v. Sears, Roebuck & Co.</i> , 421 U.S. 132 (1975)	21, 37, 41
<i>PHE, Inc. v. Dep't of Justice</i> , 983 F.2d 248 (D.C. Cir. 1993)	<i>passim</i>

<i>Pickering v. Board of Educ.</i> , 391 U.S. 563 (1968).....	31
<i>Rosenfeld v. United States Dep’t of Justice</i> , 57 F.3d 803 (9th Cir. 1995)	<i>passim</i>
<i>SafeCard Services, Inc. v. SEC</i> , 926 F.2d 1197 (D.C. Cir. 1991).....	<i>passim</i>
<i>Schiller v. NLRB</i> , 964 F.2d 1205 (D.C. Cir. 1992).....	30
<i>Schlefer v. United States</i> , 702 F.2d 233 (D.C. Cir. 1983).....	22, 39
<i>In re Sealed Case</i> , 146 F.3d 881, 885 (D.C. Cir. 1998).....	14, 30
<i>In re Sealing and Non-Disclosure of Pen/Trap/2703(d) Orders</i> , 562 F. Supp. 2d 876 (S.D. Tex. 2008).....	7
<i>Senate of Puerto Rico v. United States Dep’t of Justice</i> , 823 F.2d 574 (D.C. Cir. 1987).....	25
<i>South-Central Timber Development, Inc. v. Wunnicke</i> , 467 U.S. 82 (1984).....	31
<i>State of Maine v. United States Dep’t of Interior</i> , 298 F.3d 60 (1st Cir. 2002).....	56, 57
<i>Tracey v. State</i> , 152 So. 3d 504 (Fla. 2014)	6
<i>United States Dep’t of State v. Ray</i> , 502 U.S. 164 (1991).....	23
<i>United States v. Bus. Of the Custer Battlefield Museum & Store</i> , 658 F.3d 1188 (9th Cir. 2011)	15, 40
<i>United States v. Davis</i> , 785 F.3d 498 (11th Cir. 2015) (en banc)	6

United States v. Jones,
 —U.S.—, 132 S. Ct. 945 (2012).....*passim*

Voinche v. FBI,
 412 F. Supp. 2d 60 (D.D.C. 2006).....44

Wickline v. FBI,
 No. 92-1189, 1994 WL 549756 (D.D.C. Sept. 30, 1994)54

Wiener v. FBI,
 943 F.2d 972 (9th Cir. 1991)23, 36, 46, 51

Yonemoto v. Dep’t of Veterans Affairs,
 686 F.3d 681 (9th Cir. 2011)21

Statutes

5 U.S.C. § 552(a)(1)-(2).....20

5 U.S.C. § 552(a)(3).....20

5 U.S.C. § 552(a)(6)(E).....10

5 U.S.C. § 552(b)21, 55

5 U.S.C. § 552(b)(3).....16

5 U.S.C. § 552(b)(7).....14, 19, 45

5 U.S.C. § 706(2)39

18 U.S.C. § 2703(d)12

18 U.S.C. § 3123(d)16, 52

Freedom of Information Act*passim*

Congressional Materials

H.R. 656, 114th Cong. (1st Sess. 2015).....6

H.R. Rep. No. 93-876 (1974), *reprinted in* 1974 U.S.C.C.A.N. 626757

S. Rep. No. 93-1200 (1974) (Conf. Rep.), *reprinted in*
 1974 U.S.C.C.A.N. 628543, 50

Rules

Fed. R. Civ. P. 26(b)(3).....	24
Fed. R. Civ. P. 56	56

Other Authorities

Davis, <i>The Information Act: A Preliminary Analysis</i> , 34 U. Chi. L. Rev. 761, 797 (1967)	21
<i>Definition of Telematics</i> , PC Magazine	5
Ellen Nakashima, <i>Little-Known Surveillance Tool Raises Concerns by Judges, Privacy Activists</i> , Wash. Post, Mar. 27, 2013.....	9
Jennifer Steinhauer and Jonathan Weisman, <i>U.S. Surveillance in Place Since 9/11 Is Sharply Limited</i> , N.Y. Times, June 2, 2015.....	7
John Shiffman and Kristina Cooke, <i>Exclusive: U.S. Directs Agents to Cover Up Program Used to Investigate Americans</i> , Reuters, Aug. 5, 2013.....	9, 39
April A. Otterberg, <i>GPS Tracking Technology: The Case for Revisiting Knotts and Shifting the Supreme Court’s Theory of the Public Space Under the Fourth Amendment</i> , 46 B.C. L. Rev. 661, 680-83 (2005)	8
Pew Research Ctr., Mary Madden, <i>Public Perceptions of Privacy and Security in the Post-Snowden Era</i> , Pew Research Ctr., 32, 34 (Nov. 12, 2014).....	6
Stephen Wm. Smith, <i>Gagged, Sealed & Delivered: Reforming ECPA’s Secret Docket</i> , 6 Harv. L. & Pol’y Rev. 313, 322 (2012).....	7

INTRODUCTION

This appeal involves the public’s right to know what the government is doing and why. The Department of Justice seeks to withhold guidance documents that instruct federal prosecutors about the type of court authorization, if any, the Department contends is necessary before it uses surveillance technologies that allow it to track a person’s location. Information about the legal safeguards followed by the government when using these technologies would shed light on urgent public and legislative debates about surveillance and privacy. But it is nearly impossible for the public to obtain this information, in part because the government seeks court authorization to conduct this type of surveillance in sealed, *ex parte* proceedings that typically remain under seal forever.

In enacting the Freedom of Information Act, Congress sought to pierce the veil of administrative secrecy. A core feature of the statutory scheme is the prohibition against secret agency law: Agencies may not create “working law,” informal rules or policies governing the exercise of their official functions, but then hide them from public view. When it comes to the deployment of location tracking technology, however, the government has done just that. DOJ’s guidance documents tell federal prosecutors what kind of court approval, if any, DOJ contends is necessary before the government can surveil someone’s whereabouts.

These documents reflect the agency's "working law" and are exactly the type of information agencies must disclose.

To justify withholding these documents, DOJ invokes FOIA's Exemption 5, which incorporates the attorney work-product privilege, and Exemption 7(E), which protects law enforcement techniques and guidelines where disclosure would allow people to circumvent the law. The district court correctly concluded that the government did not meet its burden of proving either exemption.

The guidance documents are not protected work product because they set forth general legal guidelines, and lack any analysis of the facts relating to any specific case or enforcement action. The district court adopted the D.C. Circuit's rule that when the government acts in its sovereign capacity to enforce the law, it must show that documents were prepared in connection with a specific claim to establish the work-product privilege. This rule, derived from a consistent line of cases, sensibly balances the government's litigation needs, by allowing it to withhold documents prepared in anticipation of litigating specific cases, with the public's interest in learning the official positions staked out by the government when it exercises its sovereign power to enforce the law. This rule also recognizes that when the government acts more like a private entity, defending itself against potential liability, it should benefit from the same work-product privilege as

ordinary litigants. As a result, the specific-claim requirement does not apply in those circumstances.

Nor are these guidance documents protected by Exemption 7(E). Although the government asserts that they contain “details” not known by the public about location tracking technologies, it fails to explain why disclosure of these details would create a risk of circumvention. Indeed, they would not. The “details” here involve the legal standards used by the government before engaging in surveillance. That is not the type of information protected from disclosure by Exemption 7(E).

In short, disclosure of the government’s legal standards for deploying surveillance technology would not harm the interests underlying the work-product privilege or Exemption 7(E), but would further FOIA’s core purpose in exposing agency action to the light of public scrutiny.

JURISDICTIONAL STATEMENT

Plaintiffs¹ concur in Defendant’s jurisdictional statement.

¹ The parties are filing concurrently with this brief a joint motion to dismiss Plaintiff-Appellee *San Francisco Bay Guardian* from this appeal. The *San Francisco Bay Guardian* has ceased operating a newspaper and was dismissed from the district court proceedings after the government filed the notice of appeal. See ER 100 (Docket Entry 72). The Court has not yet had an opportunity to rule on the motion to dismiss, and so this brief is submitted on behalf of both Plaintiffs-Appellees.

ISSUES PRESENTED

1. Is a manual for federal prosecutors, setting forth legal guidelines governing the use of location tracking technologies, attorney work product exempt from disclosure under FOIA's Exemption 5?
2. Does this same manual reflect law enforcement techniques or guidelines that, if disclosed, would risk circumvention, making it exempt from disclosure under FOIA's Exemption 7(E)?

STATEMENT OF FACTS

A. The Public Has a Significant Interest in Learning about the Government's Location Tracking Policies and Procedures

“Recent years have seen the emergence of many new devices that permit the monitoring of a person's movements.” *United States v. Jones*, __U.S.__, 132 S. Ct. 945, 963 (2012) (Alito, J., concurring). Advances in new technology “make long-term monitoring relatively easy and cheap.” *Id.* at 964. But such monitoring also raises privacy concerns because it “generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations.” *Id.* at 955 (Sotomayor, J., concurring).

Resolving a split in the federal courts of appeal, the Supreme Court unanimously held in *Jones* that use of a Global Positioning System (“GPS”) device to track a suspect's vehicle constitutes a “search” within the meaning of the Fourth

Amendment. *See id.* at 949; *id.* at 954 (Sotomayor, J., concurring); *id.* at 964 (Alito, J., concurring). But GPS is only one of many techniques available to the government to track location. These include requests to wireless carriers for cellular telephone location information, SER 132-35; “cell site simulators,” which mimic cell towers and force telephones to relay location and other information directly to the government’s device, SER 115, 179-232; and access to “Telematics Providers,” which are on-board vehicular navigation systems, SER 172-177.²

Each of these location tracking technologies raises critical questions of fact, law, and policy.

What legal protocols does the government follow before conducting the surveillance: Does it seek *any* court approval to use the technique? With at least some of these technologies, the government has taken the position that it needs no court authorization at all. SER 115, 118 (DOJ’s position between 1994 and 2001 was that government could use cell site simulators to track a suspect’s location without any court authorization). But when it does obtain prior court approval,

² “Originally coined to mean the convergence of telecommunications and information processing, the term later evolved to refer to automation in automobiles. GPS navigation, integrated hands-free cellphones, wireless communications and automatic driving assistance systems all come under the telematics umbrella. General Motor’s OnStar was the first to combine GPS with roadside assistance and remote diagnostics.” *Definition of Telematics*, PC Magazine, <http://www.pcmag.com/encyclopedia/term/52693/telematics> (last visited June 19, 2015).

what type of court authorization does it seek – statutory court orders or warrants based on a higher probable cause showing?

And what type of court authorization *should* it seek? Except for GPS, which was resolved by the Supreme Court in *Jones*, that question is unresolved for each of the many location tracking technologies used by the government.³

Finally, do the government's practices reflect societal sentiment on the privacy safeguards that should be in place before such surveillance is conducted?

The answers to these questions would shed light on urgent, pending debates over privacy and government surveillance. Recent polling data show that people consider their location information to be highly private—more sensitive even than the contents of their text messages, a list of websites they have visited, or their relationship history.⁴ And elected officials have repeatedly considered legislation to regulate the government's access to location information.

See, e.g., Online Communications and Geolocation Protection Act, H.R. 656,

³ Appellate courts are divided, for example, on whether a request to a wireless carrier for a cellular telephone user's historical location information requires a warrant, or can instead be obtained on a lesser statutory showing. *Compare, e.g., Tracey v. State*, 152 So. 3d 504, 526 (Fla. 2014) (requiring a warrant), *with, e.g., United States v. Davis*, 785 F.3d 498 (11th Cir. 2015) (en banc) (holding that collection of phone records is not a search for which a warrant is required). The Ninth Circuit has yet to decide the issue.

⁴ Pew Research Ctr., Mary Madden, *Public Perceptions of Privacy and Security in the Post-Snowden Era*, Pew Research Ctr., 32, 34 (Nov. 12, 2014), *available at* http://www.pewinternet.org/files/2014/11/PI_PublicPerceptionsofPrivacy_111214.pdf.

114th Cong. (1st Sess. 2015). Indeed, recent experience demonstrates that public disclosure of the government's surveillance practices can prompt dramatic legislative change. *See, e.g.,* Jennifer Steinhauer and Jonathan Weisman, *U.S. Surveillance in Place Since 9/11 Is Sharply Limited*, N.Y. Times, June 2, 2015, available at www.nytimes.com/2015/06/03/us/politics/senate-surveillance-bill-passes-hurdle-but-showdown-looms.html (noting that passage of the USA FREEDOM Act signaled a “shift against the security state [that] began with the revelation by Edward J. Snowden, a former National Security Agency contractor, about the bulk collection of phone records”).

B. The Public Faces Significant Barriers to Obtaining Information about the Legal Safeguards Followed by the Government

Basic information about the legal safeguards followed by the government before obtaining location information is necessary for meaningful public and legislative debate, but hard to come by.

This is so in large part because the federal government typically obtains electronic surveillance orders *ex parte* and under seal, and those orders often remain sealed indefinitely. *See In re Sealing and Non-Disclosure of Pen/Trap/2703(d) Orders*, 562 F. Supp. 2d 876, 878 (S.D. Tex. 2008) (3,886 electronic surveillance orders issued under seal in Southern District of Texas between 1995 and 2007, 99.7% of which “remain[ed] under seal [in 2008], many years after [their initial] issuance”); Stephen Wm. Smith, *Gagged, Sealed &*

Delivered: Reforming ECPA's Secret Docket, 6 Harv. L. & Pol'y Rev. 313, 322 (2012) (estimating that federal magistrate judges issued more than 30,000 orders for electronic surveillance under seal in 2006, “more than thirty times the annual number of [Foreign Intelligence Surveillance Act] cases”).

Judicial opinions may shed light on legal protocols followed by the government when using particular location tracking techniques. But these issues typically arise in motions to suppress in criminal proceedings. Such opinions are often rendered years after the technique was deployed in the particular case, and potentially decades after the government began deploying the technique. *See, e.g., Jones*, 132 S. Ct. at 963 (deciding in 2012 that use of GPS device to track a suspect's vehicle in 2005 constituted a search for which a warrant was presumptively required); April A. Otterberg, *GPS Tracking Technology: The Case for Revisiting Knotts and Shifting the Supreme Court's Theory of the Public Space Under the Fourth Amendment*, 46 B.C. L. Rev. 661, 680-83 (2005) (government used GPS to track suspects' vehicles starting at least in 1997).

Moreover, some technologies might never come before the courts. Troubling reports suggest that the government may not be revealing to the judiciary the true nature of the electronic surveillance it conducts. For example, federal investigators have “routinely used a sophisticated surveillance system to scoop up data from cellphones and other wireless devices in an effort to track

criminal suspects — but failed to detail the practice to judges authorizing the probes.” Ellen Nakashima, *Little-Known Surveillance Tool Raises Concerns by Judges, Privacy Activists*, Wash. Post, Mar. 27, 2013, available at http://www.washingtonpost.com/world/national-security/little-known-surveillance-tool-raises-concerns-by-judges-privacy-activists/2013/03/27/8b60e906-9712-11e2-97cd-3d8c1afe4f0f_story.html.

Equally troubling, the Drug Enforcement Agency has obtained information from national security databases for use in its investigations, but instructed its investigators to conceal the source of that information from courts, instead inventing a seemingly legitimate investigative trail under a process known as parallel construction. *See, e.g.*, John Shiffman and Kristina Cooke, *Exclusive: U.S. Directs Agents to Cover Up Program Used to Investigate Americans*, Reuters, Aug. 5, 2013, available at <http://www.reuters.com/article/2013/08/05/us-dea-sod-idUSBRE97409R20130805>. This has allowed the government to conceal its use of these technologies, even when relying on their fruits to bring criminal charges.

C. Plaintiffs Submitted a FOIA Request for Information about DOJ’s Location Tracking Policies and Procedures

In light of these barriers to obtaining accurate, timely, or complete information about the government’s use of location tracking technologies, Plaintiffs American Civil Liberties Union of Northern California and the *San*

Francisco Bay Guardian, a civil rights organization and an independent newspaper, respectively, submitted a FOIA request in April 2012 seeking records pertaining to the government's policies and procedures on location tracking, as well as actual applications for court orders or warrants for location information. Specifically, the FOIA request sought:

- 1) All requests, subpoenas, and applications for court orders or warrants seeking location information since January 1, 2008.
- 2) Any template applications or orders that have been utilized by United States Attorneys in the Northern District [of California] to seek or acquire location information since January 1, 2008.
- 3) Any documents since January 1, 2008, related to the use or policies of utilizing any location tracking technology, including but not limited to cell-site simulators or digital analyzers such as devices known as Stingray, Triggerfish, AmberJack, KingFish or Loggerhead.
- 4) Any records related to the Supreme Court's holding in *United States v. Jones*, excluding pleadings or court opinions filed in the matter in the Supreme Court or courts below.

ER 77. DOJ granted Plaintiffs' request for expedited processing, pursuant to 5 U.S.C. § 552(a)(6)(E). ER 90. After receiving no response to the FOIA request, Plaintiffs filed suit on July 31, 2012. ER 64.

Based on the parties' stipulation, the Court bifurcated the issues for summary judgment and separately addressed the request for actual applications for court orders or warrants (request one) and the requests for policies and procedures

(requests two through four). SER 237-38. The district court's ruling on the requests for policies and procedures forms the basis for this appeal.

D. DOJ Withheld Documents Pursuant to FOIA's Exemption 5 and 7(E)

In response to Plaintiffs' requests for policies and procedures, the government produced some documents but withheld others, asserting them to be exempt from disclosure pursuant to FOIA's Exemption 5, as attorney work product, and Exemption 7(E) for law enforcement techniques. ER 3-4, 7.

The withheld documents include (1) template applications and orders (referred to below as EOUSA 1), (2) two excerpts from the "USABook" (referred to below as CRM Four and Five), and (3) three memos analyzing the implications for pending litigation of *Jones* and another court decision, *In re Application*, 534 F. Supp. 2d 585 (W.D. Pa. 2008) ("*In re Application*") (referred to below as CRM One, Two, and Three). ER 12-13, 42-43.

Templates. Upon review of the record, the court below found that the templates did "not provide legal theories or strategies for use in criminal litigation. Rather, they instruct government attorneys on how to apply for an order for location tracking information." ER 14.

USABook. The USABook is "a legal resource book or reference guide for federal prosecutors." ER 32. It contains "up-to-date legal analysis and guidance of specific legal topics germane to federal prosecutors." ER 32.

The two excerpts of the USABook discuss various forms of tracking location through cellular phones and vehicles. One of the documents, CRM Four, discusses “Obtaining Location Information from Wireless Carriers,” “Mobile Tracking Devices,” and “Telematics Providers (OnStar, etc.).” ER 50. The other USABook excerpt, CRM Five, “discusses electronic tracking devices generally and cellular telephone location information.” ER 57.

CRM Four and Five discuss the type of court authorization that DOJ contends is necessary and/or sufficient for the government to engage in these forms of location tracking. This is evidenced by the fact that the USABook contains template applications for various types of court orders. *See, e.g.*, ER 32 (USABook “contains an appendix with forms or go-bys useful to federal prosecutors”); ER 54 (template application pursuant to 18 U.S.C. § 2703(d) to obtain historical cell site records from wireless provider); ER 55 (template application pursuant to Pen Register Statute to obtain location information from iridium satellite telephone).

Based on this record, the court found that the USABook “function[s] like an agency manual, providing instructions to prosecutors on how to obtain location information.” ER 20.

Jones and In re Application memos. The memos, CRM One, Two, and Three, discuss the implications of two court decisions. They “assess the strengths

and weaknesses of alternative litigating positions” and offer “recommendations” to prosecutors. ER 31.

E. The Decision Below

The district court held that the templates and USABook excerpts do not constitute attorney work product because they provide general guidelines and do not pertain to specific claims. ER 14-16, 20. The court relied on D.C. Circuit caselaw, including *Jordan v. United States Dep’t of Justice*, 591 F.2d 753 (D.C. Cir. 1978), which held that a portion of the United States Attorney’s Manual and guidelines relating to the exercise of prosecutorial discretion did not constitute work product subject to Exemption 5 because they were “promulgated as general standards to guide the Government lawyers,” and did not contain the type of “factual information, mental impressions,” and “legal theories or strategies” relevant to a “particular trial” that the work-product privilege was intended to protect. ER 13-14 (citing *Jordan*, 591 F.2d at 775, 776); *see also id.* at 15 (quoting *Coastal States Gas Corp. v. Dep’t of Energy*, 617 F.2d 854 (D.C. Cir. 1980)). In so ruling, the court rejected DOJ’s argument that it was not required to prove a specific claim to establish the privilege in this case. ER 15. Relying on another D.C. Circuit decision, the court explained that the specific-claim test applies when “government lawyers are acting as ‘prosecutors or investigators of suspected wrongdoers,’” but not when they “act ‘as legal advisors protecting their agency

clients from the possibility of future litigation.” ER 15 (quoting *In re Sealed Case*, 146 F.3d 881, 885 (D.C. Cir. 1998)).

At the same time, the court found the *Jones* and *In re Application* memos to be protected work product because, unlike “an agency manual” that “convey[s] routine agency policy,” they were “more pointed” documents. ER 19. The court also rejected Plaintiffs’ argument that the templates, USABook, and *Jones/In re Application* memos constituted the agency’s “working law” and were thus subject to disclosure. ER 11.

With respect to Exemption 7(E) for “records or information compiled for law enforcement purposes” that “would disclose techniques and procedures for law enforcement investigations or prosecutions,” 5 U.S.C. §552(b)(7), the court below concluded that the government failed to meet its burden. ER 25.

It relied on this Court’s decision in *Rosenfeld v. United States Dep’t of Justice*, 57 F.3d 803, 815 (9th Cir. 1995), which held that Exemption 7(E) only exempts investigative techniques that are not generally known to the public. ER 21. The court found that the surveillance techniques discussed in these documents are known to the public. ER 22-23. Although the government’s declarations state that the specifics on how and when the techniques are used are not generally known, the court found these conclusory assertions not sufficient to meet the government’s burden of explaining why disclosure, under these circumstances,

risks circumvention. ER 23-24. For example, “the public is already aware that minimizing vehicular or cell phone usage will allow them to evade detection.” ER 24.

The court below thus ordered disclosure of the templates (EOUSA 1) and USABook excerpts (CRM Four and Five), but not the *Jones* and *In re Application* memos (CRM One, Two, and Three). ER 26. The government seeks review of the district court’s disclosure order.⁵

F. Applications for Location Tracking Orders Filed in Court by the U.S. Attorney’s Office are Sealed Indefinitely

In addition to seeking information related to policies and procedures on location tracking, Plaintiffs also sought applications for location tracking orders or warrants, filed in court by the U.S. Attorney’s Office for the Northern District of California. ER 77. Plaintiffs did not seek records from open investigations and challenged the withholding only of court filings from closed matters. SER 12; *cf. United States v. Bus. Of the Custer Battlefield Museum & Store*, 658 F.3d 1188, 1192 (9th Cir. 2011) (after close of investigation, search warrant materials constitute judicial records to which public has common law right of access).

⁵ The government has since produced to Plaintiffs the templates contained in EOUSA 1 and CRM Four. The narrative portions of CRM Four and Five remain at issue on this appeal.

The government initially identified 760 matters as potentially involving location tracking; all but six were sealed. SER 40-41. After eliminating unsealed files (which the government produced) and files related to open investigations, the remaining files numbered 349. SER 29-30, 40-42.

The government contended that it was not required to review and process, let alone disclose, the remaining files because they were all under seal. SER 16. It explained that “[w]hen using investigative tools such as applying for an order seeking location tracking information, the general practice at the [United States Attorney’s Office] is also to apply to seal the application (if any), affidavit (if any) and order.” SER 35.

It further explained that once these court filings are placed under seal, they effectively remain under seal forever. This is so because “[t]here is no systematic review on an ongoing basis of the sealed applications to determine whether the conditions requiring sealing continue.” SER 36.

The district court held that the government was required to review and process the files, but any court applications filed pursuant to the Pen Register Statute, 18 U.S.C. § 3123(d), would be exempt from disclosure under FOIA’s Exemption 3. *See* 5 U.S.C. § 552(b)(3) (information prohibited from disclosure by another statute exempt from disclosure under FOIA); SER 26. It also held that to the extent there were any remaining files (*i.e.*, applications not filed pursuant to the

Pen Register Statute), the government had to “separately justify the reason(s) the record(s) remain under seal.” SER 22; *see Morgan v. United States Dep’t of Justice*, 923 F.2d 195, 199 (D.C. Cir. 1991) (holding that “the mere existence of a court seal is, without more, insufficient to justify nondisclosure under the FOIA”).⁶

STANDARD OF REVIEW

A district court’s legal rulings on summary judgment in a FOIA matter are reviewed *de novo*. *Rosenfeld*, 57 F.3d at 807. This Court applies “a special standard to review factual issues”: “Instead of determining whether a genuine issue of material fact exists, we employ the following two-step standard. We inquire whether an adequate factual basis supports the district court’s ruling. If such a basis exists, we overturn the ruling only if it is clearly erroneous.” *Id.*

This Court “may affirm a district court’s judgment on any ground supported by the record, whether or not the decision of the district court relied on the same grounds or reasoning.” *Atel Fin. Corp. v. Quaker Coal Co.*, 321 F.3d 924, 926 (9th Cir. 2003).

SUMMARY OF ARGUMENT

The government did not meet its burden of establishing either the work-product privilege or Exemption 7(E).

⁶ The parties have reached a settlement in principle to resolve Plaintiffs’ request for applications for court orders or warrants. SER 2.

The district court correctly held that where, as here, the government acts in its capacity to enforce the law, it must demonstrate that a document was prepared in anticipation of litigating a specific claim based on concrete facts to invoke the work-product privilege.

Although DOJ complains that the specific-claim requirement is too onerous and should not be applied to the government's criminal litigation, the rule applied by the court below finds support in a consistent line of cases and recognizes the important distinction between the government acting in its sovereign capacity to enforce the law and the government asserting its proprietary interests in defending itself from liability. The law imposes greater restraints on the sovereign in a variety of contexts and it is logical for the work-product doctrine to do the same.

The documents at issue in this case are excerpts from the USABook, a manual for federal prosecutors that contains legal standards governing the use of location tracking technologies in criminal investigations and prosecutions. They reflect the exercise of a core sovereign function – investigating and prosecuting criminal violations – and they set forth general standards, outside the context of any particular case. The district court correctly concluded that the specific-claim requirement applies in this case, and that the documents do not constitute attorney work product.

Even if the specific-claim requirement does not apply, however, the district court should still be affirmed. The USABook functions like an agency manual and DOJ has not met its burden of demonstrating that it contains the type of strategic analysis the work-product privilege was intended to protect.

Moreover, FOIA's working law doctrine confirms the conclusion that the USABook is not privileged. The doctrine is intended to prevent agencies from conducting government business pursuant to secret rules or procedures. A manual setting forth the legal safeguards used by the government before deploying surveillance technologies is exactly the kind of secret agency law that must be disclosed under FOIA.

Nor has DOJ met its burden of establishing that the documents fall under Exemption 7(E), for techniques and guidelines, disclosure of which risks "circumvention of the law." *See* 5 U.S.C. § 552(b)(7)(E). Although the government contends that the district court created a categorical rule that Exemption 7(E) is unavailable whenever some aspect of the technique has become public, this mischaracterizes the decision below, which merely held the government to its burden of demonstrating circumvention.

Indeed, it is the government that seeks to create a categorical rule that it can seek shelter in Exemption 7(E) simply by stating that the documents discuss unspecified "details" or "circumstances" of a technique's use. Even the cases on

which DOJ relies make clear that the government must describe the “details” with sufficient specificity to allow a meaningful assessment of whether disclosure risks circumvention. Here, the government makes the conclusory assertion that disclosure of “details” would risk circumvention, without explaining why or how that is the case. Nor is any such explanation self-evident. To the contrary, the withheld documents pertain to the legal safeguards observed by the government before deploying location tracking technology. Disclosure of the government’s position regarding its own statutory and constitutional obligations does not create a risk of circumvention. It keeps the government accountable to the public.

ARGUMENT

I. Exemption 5 Does not Shield from Disclosure a Manual for Prosecutors Setting Forth Legal Standards

A. FOIA Favors Disclosure over Secrecy

Congress enacted FOIA “to pierce the veil of administrative secrecy and to open agency action to the light of public scrutiny.” *Dep’t of Air Force v. Rose*, 425 U.S. 352, 361 (1976) (internal quotation marks, citation omitted). FOIA affirmatively requires agencies to make public specified categories of documents. *See* 5 U.S.C. § 552(a)(1)-(2) (2011). Documents that do not fall within FOIA’s affirmative provision must also be made available to the public, unless they fall within one or more of FOIA’s nine statutory exemptions from disclosure. *See id.* at §§ 552(a)(3) & (b)(1)-(9). An agency may withhold only the information to

which an exemption applies, and must release all “reasonably segregable” non-exempt information. 5 U.S.C. § 552(b).

FOIA’s purpose of promoting government transparency is reflected in several facets, both substantive and procedural, of the statutory scheme.

First, FOIA “represent[s] a strong congressional aversion to ‘secret (agency) law.’” *NLRB v. Sears, Roebuck & Co.*, 421 U.S. 132, 153 (1975) (quoting Davis, *The Information Act: A Preliminary Analysis*, 34 U. Chi. L. Rev. 761, 797 (1967)). The statute’s “core purpose” is to inform citizens about “what their government is up to.” *Yonemoto v. Dep’t of Veterans Affairs*, 686 F.3d 681, 687 (9th Cir. 2011) (citation omitted). As a matter of substantive law, the statute thus requires the disclosure of an agency’s “working law,” which includes “the agency’s effective law and policy,” as well as “the reasons which . . . suppl[ied] the basis for an agency policy actually adopted.” *Sears*, 421 U.S. at 152-53. When an agency “actually adopt[s]” a policy, that policy position and the “reasons” underlying it “constitute the ‘working law’ of the agency” and must be disclosed. *Id.* at 152-53.

The working law doctrine thus furthers FOIA’s central premise – “that the public is entitled to know what its government is doing and why.” *Coastal States*, 617 F.2d at 868. Agencies are not permitted to develop *de facto* policies and procedures, but avoid disclosure by characterizing them as unofficial. “A strong theme of our opinions has been that an agency will not be permitted to develop a

body of ‘secret law,’ used by it in the discharge of its regulatory duties and in its dealings with the public, but hidden behind a veil of privilege because it is not designated as ‘formal,’ ‘binding,’ or ‘final.’” *Id.* at 867; *see also Assembly of State of California v. United States Dep’t of Commerce*, 968 F.2d 916, 920 (9th Cir. 1992) (“working law” doctrine “insures that the agency does not operate on the basis of ‘secret law’”).

Applying these principles, courts have repeatedly rejected efforts to withhold documents setting forth an agency’s legal position. *See, e.g., Coastal States*, 617 F.2d at 857-58, 869 (memoranda setting forth “interpretations of regulations”); *Schlefer v. United States*, 702 F.2d 233, 235, 245 (D.C. Cir. 1983) (opinions of the Chief Counsel of the Maritime Administration interpreting three statutes). Notably, the working law doctrine applies even when the agency policy pertains directly to litigation. *See Jordan*, 591 F.2d at 755, 772 (requiring disclosure of manual for federal prosecutors and guidelines relating to exercise of prosecutorial discretion).⁷

⁷ In addition to Exemption 5, *Jordan* addressed Exemption 2, which covers “personnel rules and practices” and is not at issue here. *Id.* at 763 (quoting 5 U.S.C. § 552(b)(2)). The D.C. Circuit subsequently rejected *Jordan*’s analysis of Exemption 2. *See Crooker v. Bureau of Alcohol, Tobacco & Firearms*, 670 F.2d 1051, 1073 (D.C. Cir. 1981). But *Crooker* left undisturbed *Jordan*’s Exemption 5 analysis. Moreover, *Crooker* was subsequently abrogated by the Supreme Court’s decision in *Milner v. Dep’t of Navy*, 562 U.S. 562 (2011).

Second, because “disclosure, not secrecy, is the dominant objective of the Act,” FOIA’s exemptions “must be narrowly construed.” *Rose*, 425 U.S. at 361; accord *Kamman v. IRS*, 56 F.3d 46, 48 (9th Cir. 1995); *Church of Scientology of California v. United States Dep’t of Army*, 611 F.2d 738, 742 (9th Cir. 1979).

Third, the government bears the burden of proving the applicability of an exemption. *United States Dep’t of State v. Ray*, 502 U.S. 164, 173 (1991); see also *Minier v. Central Intelligence Agency*, 88 F.3d 796, 800 (9th Cir. 1996).

Fourth, in meeting its burden, “the government may not rely upon conclusory and generalized allegations of exemptions.” *Church of Scientology*, 611 F.2d at 742 (internal quotation marks, citation omitted). The agency cannot rely on unsupported assertions that disclosure will or may result in a particular consequence, and must instead provide sufficient information “to afford the FOIA requester a meaningful opportunity to contest, and the district court an adequate foundation to review, the soundness of the withholding.” *Wiener v. FBI*, 943 F.2d 972, 977 (9th Cir. 1991) (internal quotation marks, citation omitted).

Particularized information is necessary to minimize distortions in the adversary process inherent in FOIA litigation, in which “only the party opposing disclosure will have access to all the facts.” *Id.* at 977.

B. General Legal Protocols for Using Location Tracking Technologies Do not Constitute Attorney Work Product

The district court correctly found that the USABook does not constitute attorney work product because it was not generated in connection with a specific claim based on concrete facts. The specific-claim requirement applied by the court below rests on consistent caselaw and sound logic. In any event, the USABook would not be protected work product, even if the specific-claim requirement does not apply.

1. Courts in FOIA Cases Consistently Require the Government to Demonstrate a Specific Claim to Establish the Work-Product Privilege

The purpose of the work-product privilege is to protect the adversary process by shielding the “mental impressions of an attorney” in the “preparation of a client’s case.” *Hickman v. Taylor*, 329 U.S. 495, 510, 511 (1947); *see also Holmgren v. State Farm Mut. Auto. Ins. Co.*, 976 F.2d 573, 576 (9th Cir. 1992) (“The primary purpose of the work product rule is to prevent exploitation of a party’s efforts in preparing for litigation.”) (citation omitted). This means that “[t]he work-product rule does not extend to every written document generated by an attorney.” *Coastal States*, 617 F.2d at 864 (citation omitted). Instead, a document enjoys the work-product privilege only if it is “prepared in anticipation of litigation.” *See* Fed. R. Civ. P. 26(b)(3). This limitation is critical to the work-product doctrine and to the purposes of FOIA: “While it may be true that the

prospect of future litigation touches virtually any object of a DOJ attorney's attention, if the agency were allowed 'to withhold any document prepared by any person in the Government with a law degree simply because litigation might someday occur, the policies of the FOIA would be largely defeated.'" *Senate of Puerto Rico v. United States Dep't of Justice*, 823 F.2d 574, 586-87 (D.C. Cir. 1987) (citation omitted).

To avoid this unintended consequence, the D.C. Circuit has construed this requirement in the FOIA context to mean that "[t]he documents must at least have been prepared with a *specific claim* supported by *concrete facts* which would likely lead to litigation." *Coastal States*, 617 F.2d at 865 (emphasis added). *Coastal States* thus held that government attorneys' interpretations of agency regulations provided to agency staff conducting regulatory compliance audits were not protected work product where the agency "neglected to supply the court with sufficient facts . . . to permit a conclusion that in fact specific claims had arisen." *Id.* at 857-58, 866. It therefore affirmed an order requiring disclosure of these documents. *Id.* at 870-71.

The court in *SafeCard Services, Inc. v. SEC*, 926 F.2d 1197 (D.C. Cir. 1991), further elaborated on the specific-claim requirement:

A law enforcement agency may meet this standard by demonstrating that one of its lawyers prepared a document in the course of an investigation that was undertaken with litigation in mind. Such an investigation would have to be, and typically would be, based upon a suspicion of specific wrongdoing

and represent an attempt to garner evidence and to build a case against the suspected wrongdoer.

Id. at 1202. The SEC satisfied this standard because the SEC’s lawyers had created the document at issue “in the course of an investigation of particular subjects – individuals and companies that it believed may have violated the law.”

Id. at 1203.⁸

Notably, the D.C. Circuit in *Jordan* rejected DOJ’s work-product claim for a portion of the United States Attorney’s Manual and guidelines because they were “promulgated as *general* standards to guide the Government lawyers” in the exercise of prosecutorial discretion; they did not contain the type of “factual information, mental impressions” and “legal strategies relevant” to a “*particular* trial” that the work-product privilege was intended to protect. 591 F.2d at 775-76 (emphasis added).

⁸ The government attempts to dismiss *Coastal States* and *SafeCard* as cases in which the court “simply found” the work-product privilege satisfied where a specific claim was involved. See Appellant’s Opening Brief (“AOB”) at 30. This misrepresents the holding of *Coastal States*, which found some documents protected where the government established a specific claim, and others unprotected where it had not. See *Coastal States*, 617 F.2d at 865, 866. The court’s “specific claim” language was thus necessary to the decision. And while *SafeCard* found the government to have established the privilege by demonstrating that the documents were prepared in the course of investigating a particular investigation, 926 F.2d at 1203, this hardly undermines the D.C. Circuit’s consistent emphasis on the importance of a specific claim.

Jordan, *Coastal States*, and *SafeCard* thus teach that the attorney work-product privilege does not extend to general legal standards that guide agency staff, even when those standards involve interpretations or guidelines about how the law should be enforced, *see Jordan*, 591 F.2d at 775-76 (general guidelines about prosecutorial discretion); *Coastal States*, 617 F.2d at 858 (agency’s interpretations of its petroleum pricing and allocation regulations for purposes of conducting compliance audits), but does apply to documents “prepared with a specific claim supported by concrete facts which would likely lead to litigation.” *Coastal States*; 617 F.2d at 865; *see also SafeCard*, 926 F.2d at 1203 (documents prepared in the course of SEC “investigation of particular subjects”).⁹

The government contends that because *Jordan* involved documents related to prosecutorial discretion, the case stands only for the proposition that documents must have been “prepared in anticipation of actual litigation, whether or not related to a specific, identifiable investigation.” AOB at 29. But the exercise of prosecutorial discretion necessarily presupposes, and thus anticipates, that the prosecutors can initiate “actual litigation.” Indeed, guidelines concerning prosecutorial discretion turn on two of the most fundamental questions of litigation strategy – whether to bring a case at all, and, if so, what claims or charges to

⁹ The D.C. Circuit is not alone in applying the specific-claim requirement. *See Kent Corp. v. NLRB*, 530 F.2d 612, 623 (5th Cir. 1976) (documents protected by work-product privilege in FOIA case because they evaluated “specific claims”).

include. *See Jordan*, 591 F.2d at 757. Thus, *Jordan* underscores what *Coastal States* and *SafeCard* make explicit – that it is not enough for a document to anticipate actual or potential litigation in a general class of cases; it must also do so in connection with a particular claim.

District courts have followed this line of cases and ordered disclosure of an agency’s general legal standards for handling litigation but not documents that apply those standards to specific cases. *See Judicial Watch v. United States Dep’t of Homeland Security*, 926 F. Supp. 2d 121, 143-44 (D.D.C. 2013) (“agency policies and instructions regarding the exercise of prosecutorial discretion in civil immigration enforcement” subject to disclosure under FOIA, while documents setting forth “attorneys’ reasons for declining to prosecute in specific cases” properly withheld as work product); *American Immigration Council v. United States Dep’t of Homeland Security*, 905 F. Supp. 2d 206, 211, 222 (D.D.C. 2012) (documents relating to “the role of counsel in immigration proceedings” and “whether an INS regulation creates a right to counsel for people seeking admission as refugees” subject to disclosure under FOIA because they did not “ensu[e] from any ‘particular transaction’”) (citation omitted).

These cases recognize that even though “‘general standards’ to instruct” agency attorneys on how to conduct litigation “in specific categories of cases” “may be, in a literal sense, ‘in anticipation of litigation,’” such documents “simply

do[] not anticipate litigation in the way the work-product doctrine demands” unless they include “the mental impressions, conclusions, opinions, or legal theories of ... [an] agency attorney, relevant to a[] specific, ongoing or prospective case or cases.” *Judicial Watch*, 926 F. Supp. 2d at 142-43; *see also American Immigration Council*, 905 F. Supp. 2d at 222 (legal analysis that “convey[s] routine agency policies,” but does not relate to “any ‘particular transaction,’” is not covered by the work-product privilege, even if “those policies happen to apply in agency litigation”).

2. The Specific-Claim Requirement Applies Where the Government Acts to Enforce the Law

After *Coastal States* and *SafeCard*, the D.C. Circuit clarified that the specific-claim requirement applies where the government acts in its sovereign capacity to enforce the law, but not when government lawyers are providing legal advice to protect their clients from potential liability. The district court’s application of the specific-claim requirement to this case finds firm support in the caselaw and logic, and should be adopted by this Court.

The government is correct that the D.C. Circuit has declined to apply the specific-claim requirement, but it did so in cases that are distinguishable. In *Delaney, Migdail & Young v. IRS*, 826 F.2d 124 (D.C. Cir. 1987), the court held that the work-product privilege protected memos “advis[ing] the [Internal Revenue Service] of the types of legal challenges likely to be mounted against a proposed

program, potential defenses available to the agency, and the likely outcome.” *Id.* at 127. The court declined to apply the specific-claim requirement and instead focused on “the function performed by the withheld material.” *Id.* In *Schiller v. NLRB*, 964 F.2d 1205 (D.C. Cir. 1992), the D.C. Circuit also declined to apply the specific-claim requirement. It found documents to be protected work product where they discussed defense strategies for suits brought against the agency under the Equal Access to Justice Act. 964 F.2d at 1208.

In *In re Sealed Case*, 146 F.3d 881 (D.C. Cir. 1998), the D.C. Circuit reconciled the surface inconsistency between *Coastal States/SafeCard* and *Delaney/Schiller*. In *Coastal States* and *SafeCard*, the government lawyers acted as “prosecutors or investigators of suspected wrongdoers,” but in *Delaney* and *Schiller*, they acted “as legal advisors protecting their agency clients from the possibility of future litigation.” *Id.* at 885. The court in *Sealed Case* then held that no specific claim is required when the lawyer “rendered legal advice in order to protect the client from future litigation.” *Id.* Notably, the court did not revisit or otherwise reject the applicability of the *Coastal States/SafeCard* specific-claim test to situations “where government lawyers act as prosecutors or investigators of suspected wrongdoers.” *Id.*

Based on this caselaw, the district court held that “the specific-claim test applies” “when government lawyers are acting as ‘prosecutors or investigators of

suspected wrongdoers,” but not when they are advising their agency clients “as to potential legal challenges.” ER 15 (citations omitted).¹⁰ The rule adopted by the court below rests on a consistent line of cases, and finds further support in other legal doctrines.

When the government acts as a prosecutor or investigator of suspected wrongdoing, it acts as sovereign seeking to enforce the law. When by contrast it defends itself against potential liability, its interests are more akin to that of a private actor defending its proprietary interests. The distinction between the government acting in its sovereign and proprietary capacities is a familiar one, and the law places greater constraints on the government when acting as sovereign in a variety of contexts.¹¹ It makes sense for the work-product doctrine to reflect this distinction.

¹⁰ DOJ cites *National Ass’n of Criminal Defense Lawyers v. EOUSA*, No. 14-269, __F. Supp. 3d __, 2014 WL 7205392 (D.D.C. Dec 18, 2014) (“*NACDL*”), but the court in that case, like the court below, recognized that the specific-claim requirement applies to documents “prepared by government lawyers in connection with active investigations of potential wrongdoing.” *Id.* at *3.

¹¹ See, e.g., *South-Central Timber Development, Inc. v. Wunnicke*, 467 U.S. 82, 93 (1984) (“If a State is acting as a market participant, rather than as a market regulator, the dormant Commerce Clause places no limitation on its activities.”); *Pickering v. Board of Educ.*, 391 U.S. 563, 568 (1968) (“[T]he State has interests as an employer in regulating the speech of its employees that differ significantly from those it possesses in connection with regulation of the speech of the citizenry in general.”); *Building and Const. Trades Council v. Associated Builders and Contractors of Massachusetts*, 507 U.S. 218, 227 (1993) (National Labor Relations
(continued on next page)

Relatedly, requiring the government to disclose its *general* policies and guidance on the positions to be asserted in litigation furthers FOIA's purpose in ensuring that an agency does not "develop a body of 'secret law,' used by it in the discharge of its regulatory duties and in its dealings with the public." *Coastal States*, 617 F.2d at 867; *see also supra* Part I-A. Like the United States Attorney's Manual and guidelines at issue in *Jordan*, the USABook excerpts here constitute DOJ's working law. *See* 591 F.2d at 774; *infra* at Part I-C. Disclosure of DOJ's policies and procedures on the legal safeguards it follows in deploying location tracking technologies would enable the public to learn "what its government is doing and why." *Coastal States*, 617 F.2d at 868.

At the same time, the specific-claim requirement accommodates the government's litigation needs by insulating from disclosure documents developed in connection with "specific cases." *Judicial Watch*, 926 F. Supp. 2d at 143-44 (guidelines regarding exercise of prosecutorial discretion in civil immigration enforcement not work product, but documents setting forth "reasons for declining to prosecute in specific cases" were work product). Applying the specific-claim requirement to situations when government attorneys act to enforce the law balances the public's interest in "pierc[ing] the veil of administrative secrecy,"

(continued from prior page)

Act preempts action by state only when state acts as "regulator," but not when it acts as "proprietor" owning and managing property).

Rose, 425 U.S. at 361, and the government’s interest in protecting the “mental impressions” and other documents generated in the course of “[p]roper[ly] prepar[ing] . . . a client’s case.” *Hickman*, 329 U.S. at 511.

In short, when government attorneys act as legal advisors serving their agency client’s proprietary interests, the work-product privilege applicable to ordinary private litigants should apply. But a narrower privilege, applicable to the work of government attorneys acting on behalf of the sovereign, serves the public’s interest in keeping the sovereign accountable when it exercises its coercive power to enforce the law. *See NLRB v. Robbins Tire & Rubber Co.*, 437 U.S. 214, 242 (1978) (“The basic purpose of FOIA is to ensure an informed citizenry, . . . needed to . . . hold the governors accountable to the governed.”). These documents must be made available both in routine civil litigation and under FOIA. *See Rose*, 425 U.S. at 361 (because “disclosure, not secrecy, is the dominant objective of the Act,” FOIA’s exemptions “must be narrowly construed”).

3. The Specific-Claim Test Applies to this Case and Compels the Conclusion that the USABook is not Work Product

Here, the district court correctly found that the attorneys who prepared the USABook were “clearly acting as prosecutors, and not as attorneys advising an agency client on the agency’s potential liability.” ER 15. While the government correctly notes that there may be situations when these two categories overlap, *see* AOB at 24, this case raises no such ambiguity. In DOJ’s own account, the

documents address surveillance issues as they “relate to prospective federal criminal prosecutions and investigations that are within the authority of DOJ to conduct and to aid federal law enforcement personnel in conducting such prosecutions and investigations.” ER 34. CRM Four and Five were thus generated in the exercise of the sovereign’s core function of investigating and prosecuting violations of the law. DOJ can withhold the USABook as work product only if it satisfies the specific-claim requirement.

The agency does not even attempt to argue that the USABook would satisfy the specific-claim test. And it is not work product because it was not prepared “in the course of an active investigation focusing upon specific events and a specific possible violation by a specific party.” *SafeCard*, 926 F.2d at 1203.

4. The USABook Is not Work Product Even If the Specific-Claim Requirement Does not Apply

Even if the specific-claim requirement does not apply, the government has still failed to meet its burden. It has not shown that the USABook contains the type of strategic analysis protected by the privilege. The critical question is whether the document functions like “an agency manual, fleshing out the meaning of the statute” or instead contains a “more pointed” analysis setting forth an agency’s “legal vulnerabilities.” *Delaney*, 826 F.2d at 127. The latter is protected, the former is not. *Id.*

DOJ's own declaration states that the USABook "functions as a legal resource book or reference guide for federal prosecutors" that "contains up-to-date legal analysis and guidance of specific legal topics germane to federal prosecutors, designed to aid them in their current and future litigation." ER 32. Based on this record, the court below properly found that the USABook "function[s] like an agency manual, providing instructions to prosecutors on how to obtain location tracking information." ER 20.

To be sure, DOJ's declaration also states that the "USABook further discusses potential legal strategies, defenses, and arguments that might be considered by federal prosecutors with respect to electronic surveillance, tracking devices and non-wiretap electronic surveillance." ER 33. But this conclusory statement does not provide a sufficient factual basis to conclude that the USABook is work product.

Notably, DOJ's declaration uses the same boilerplate to discuss CRM One, Two, and Three, the memos that discuss the implications of the *Jones* and *In re Application* decisions. ER 31 (documents discuss "potential legal strategies, defenses, and arguments that might be considered by federal prosecutors" in light of recent court decisions). But the declaration goes on to state that these three memos "assess the strengths and weaknesses of alternative litigating positions and offer prosecutors guidance, recommendations and best practices going forward."

ER 31. Disclosure of the government's internal assessment of alternative litigating positions would allow "exploitation of . . . [its] efforts in preparing for litigation." *See Holmgren*, 976 F.2d at 576. The district court thus found CRM One, Two, and Three to be protected work product, ER 19, and Plaintiffs have not cross-appealed that decision.

But if the USABook, like the *Jones* and *In re Application* memos, evaluated the strengths and weaknesses of various legal arguments, the government could easily have said so. It did not. *See Wiener*, 943 F.2d at 977 (agency required to provide "particularized explanation" of why exemption satisfied because "only the party opposing disclosure [in a FOIA case] will have access to all the facts"). The decision below should be affirmed, even if the specific-claim requirement does not apply.¹²

¹² The court below recently issued a ruling, in a separate, but related FOIA action seeking different records related to DOJ's policies and procedures for electronic surveillance. *See American Civil Liberties Union of Northern California v. Dep't of Justice*, No. 13-cv-03127-MEJ (N.D. Cal. June 17, 2015), ECF No. 53. Applying a somewhat different analysis of the attorney work-product privilege than it did in this case and after reviewing the materials *in camera*, the court found template applications to be protected, but an excerpt from the USABook unprotected. *See id.* at 14-15, 22-23. To the extent the district court's review of documents from another proceeding is relevant here, it confirms the conclusion that the USABook is not protected work product.

C. DOJ's Position on the Legal Prerequisites for Obtaining Location Tracking Orders Constitutes the Agency's Working Law

The working law doctrine confirms the conclusion that the government's general guidelines regarding the position an agency asserts in litigation should be disclosed to the public, as long as the documents do not contain any discussion of specific cases or particular facts.¹³

The USABook constitutes the agency's working law. The court below erred in concluding otherwise. Disclosure of the government's rules for using location tracking technology is necessary to prevent the agency from making secret law.

Like the DOJ manual in *Jordan*, the USABook sets forth "instructions or guidelines issued by the U.S. Attorney and directed at his subordinates," in this case, about the types of court orders the agency contends are required in order to

¹³ Exemption 5 incorporates the attorney work-product as well as the deliberative process and attorney-client privileges. *Sears*, 421 U.S. at 149. The working law doctrine typically arises in the context of the deliberative process privilege, which the government does not invoke here. But both the attorney work-product and deliberative process privileges serve a similar purpose, protecting the integrity of an agency's decisionmaking process, the former in the context of litigation, the latter in the context of policy formulation. *See id.* at 151 (purpose of deliberative process privilege "is to prevent injury to the quality of agency decisions"). Disclosure of working law, the Supreme Court has recognized, does not impair an agency's decisionmaking process. *See Sears*, 421 U.S. at 151-52. As a result, withholding of working law does not serve the purpose of the work-product doctrine. *Cf. National Council of La Raza v. Dep't of Justice*, 411 F.3d 350, 360 (2d Cir. 2005) (agency's public incorporation of document precluded reliance on deliberative process as well as attorney-client privilege because "principal rationale" behind each privilege, to encourage frank communications, had "evaporate[d]").

use location tracking technologies. *Jordan*, 591 F.2d at 774. The USABook thus sets forth “positive rules that create definite standards for Assistant U.S. Attorneys to follow.” *Id.* And like the interpretations of regulations provided to agency staff conducting audits at issue in *Coastal States*, the USABook provides federal prosecutors with an analysis of the laws they rely upon “in the discharge of [their official] duties and in [their] dealings with the public.” 617 F.2d at 867.

It may well be that the USABook does “not *require* DOJ attorneys to make any particular arguments or follow any particular course of conduct,” and has not been adopted “as official DOJ policy” or reflect “any official interpretation of DOJ’s Fourth Amendment obligations.” ER 11 (emphasis added). But the contention that “documents are not . . . absolutely binding on [agency staff] misses the point,” as does the agency’s self-serving statement that the USABook is somehow unofficial. *Coastal States*, 617 F.2d at 869. DOJ’s stated purpose of the USABook is to serve as “a legal resource book or reference guide for federal prosecutors.” ER 32. Unless the document fails to serve its purpose, DOJ clearly expects it to be used “routinely . . . by agency staff as guidance in conducting their” investigations and litigation. *Coastal States*, 617 F.2d at 869. When “this occurs, the agency has promulgated a body of secret law which it is actually applying in its dealings with the public but which it is attempting to protect behind a label.” *Id.*; *see also Jordan*, 591 F.2d at 774 (finding guidelines and manual for

U.S. Attorneys to be working law even though “they may not be absolutely binding on each Assistant”).

The district court also found that the documents did not constitute “working law” because “[t]hey involve legal issues that will ultimately be decided by the Court, not the DOJ.” ER 10. But working law, by its nature, involves legal issues. *See, e.g., Coastal States*, 617 F.2d at 857-58, 869 (memoranda interpreting regulations); *Schlefer*, 702 F.2d at 235, 245 (opinions of the Chief Counsel of the Maritime Administration interpreting three statutes). And legal issues, by their nature, are typically decided by the courts. *See Marbury v. Madison*, 1 Cranch 137, 177 (1803) (it is “the province and duty of the judicial department to say what the law is”); 5 U.S.C. § 706(2) (Administrative Procedure Act provides judicial review of agency action).

In any event, there is a real danger that the legal issues here will evade judicial review and never see the public light of day. In the past, DOJ has instructed its attorneys that certain kinds of cell phone location surveillance do “not require any legal authorization to operate.” SER 136. In other instances, the government appears to instruct its agents to engage in “parallel construction,” hiding from defense lawyers and courts alike the surveillance that actually spawned an investigation and inventing an alternative source for the information. *See, e.g., John Shiffman and Kristina Cooke, Exclusive: U.S. Directs Agents to*

Cover Up Program Used to Investigate Americans, Reuters, Aug. 5, 2013, available at <http://www.reuters.com/article/2013/08/05/us-dea-sod-idUSBRE97409R20130805>. To the extent the USABook excerpts do the same, the government is unilaterally authorizing itself to conduct potentially intrusive surveillance on members of the public, while simultaneously preempting the judiciary from deciding whether and what legal safeguards are necessary and preventing the public from learning “what its government is doing and why.” *Coastal States*, 617 F.2d at 868. This is precisely the type of “secret law” “actually applie[d]” by an agency that the working law doctrine was intended to expose. *Id.* at 867 (internal quotation marks omitted).

Moreover, even when prosecutors do seek court authorization, the law is still secret because, as the record in this case confirms, the orders are almost always issued *ex parte* and under seal, and they remain sealed indefinitely. In this case, for example, the government has refused to disclose the applications for location tracking orders it filed in court, even in matters now closed. *See supra*, Statement of Facts, Part F. But the government has no idea if sealing is still justified. SER 36 (acknowledging that “there is no systematic review on an ongoing basis of the sealed applications to determine whether the conditions requiring sealing continue”); *but see Custer Battlefield*, 658 F.3d at 1196 (common law grants public

a presumptive right of access to search warrant materials once investigation has closed).

In short, the legal issues discussed in the documents DOJ seeks to withhold might never be decided by a court, and even if they are, the public might never gain access to those rulings. The “strong congressional aversion to ‘secret (agency) law’” reflected in FOIA demands disclosure of the agency’s policies and procedures governing location tracking. *Sears*, 421 U.S. at 153.¹⁴

II. Disclosure of Legal Standards Used to Engage in Well Known Location Tracking Techniques Does not Give Rise to a Risk of Circumvention

Nor has DOJ established Exemption 7(E). DOJ emphasizes that these documents discuss “details” about the “circumstances” in which location tracking technologies are used and of which the public is not aware. But FOIA does not create a *per se* exemption for “details.” Because the government bears the burden,

¹⁴ DOJ has produced to Plaintiffs the template applications in EOUSA 1 and CRM Four. It continues to withhold, however, the narrative portions of CRM Four and Five. Although the templates shed some light on the type of court authorization DOJ contends prosecutors should obtain to use location tracking technologies, they paint an incomplete picture of DOJ’s position. To the extent DOJ asserts that no court authorization is required for a particular location tracking technology, there would be no template. And CRM Five does not include any templates, ER 56-57, so the templates that have been produced do not shed light on the legal standards discussed in that document. Moreover, even if the templates produced a complete picture of DOJ’s position, the public is still entitled to learn “the reasons which . . . supply the basis for an agency policy actually adopted. These reasons, if expressed within the agency, constitute the ‘working law’ of the agency and . . . [are] outside the protection of Exemption 5.” *Sears*, 421 U.S. at 152-53. Those reasons are reflected in CRM Four and Five, and DOJ must disclose them.

it must still explain why disclosure of these details would risk circumvention.

Indeed, the “details” here pertain to the legal standards followed by the government before deploying location tracking technology. Far from assisting law violators evade detection, disclosure of this information serves FOIA’s goal of ensuring that the government does not make secret surveillance law. The district court correctly found that DOJ did not meet its burden.

A. Exemption 7(E) Requires the Government to Explain Why Disclosure of “Details” Risks Circumvention

Exemption 7(E) permits the government to withhold information about law enforcement techniques and guidelines if disclosure would risk circumvention.

The agency bears the burden of demonstrating a risk of circumvention and cannot rely on the unelaborated assertion that the document contains “details” or the “circumstances” of a technique’s use. Moreover, certain kinds of information – information about commonly known techniques and information about the government’s legal standards – simply do not risk circumvention and thus cannot be withheld pursuant to Exemption 7(E).

Exemption 7(E) protects only investigative techniques or procedures that are “not generally known to the public.” *Rosenfeld v. United States Dep’t of Justice*, 57 F.3d 803, 815 (9th Cir. 1995). Congress made clear when it first adopted this exemption in 1974 that it “should not be interpreted to include routine techniques

and procedures already well known to the public.” S. Rep. No. 93-1200 (1974) (Conf. Rep.), *reprinted in* 1974 U.S.C.C.A.N. 6285, 6291.

In *Rosenfeld*, this Court rejected the FBI’s effort to withhold information pursuant to 7(E) where the technique at issue was the use of pretext phone calls. “It would not serve the purposes of FOIA,” the Court explained, “to allow the government to withhold information to keep secret an investigative technique that is routine and generally known.” *Rosenfeld*, 57 F.3d at 815.

Nor was the Court persuaded by the FBI’s effort to reframe the technique at issue as a “more precise” version of what was publicly known, in particular, using “the identity of a particular individual, Mario Savio, as the pretext.” *Id.* “[S]uch reasoning,” the Court explained, would unacceptably permit “the government [to] withhold information under Exemption 7(E) under any circumstances, no matter how obvious the investigative practice at issue, simply by saying that the ‘investigative technique’ at issue is not the practice but the application of the practice to the particular facts underlying that FOIA request.” *Id.*

Other courts have similarly rejected the government’s effort to invoke Exemption 7(E) by relying on the unadorned claim that the documents describe the manner in which an otherwise commonly known technique is used. In *Davin v. United States Dep’t of Justice*, 60 F.3d 1043 (3d Cir. 1995), the FBI sought to withhold information about the otherwise well known technique of using

informants. It claimed “the circumstances surrounding” the use of this technique, in particular, “the manner in which informants are identified, recruited, cultivated and handled by the FBI,” were “not well-known.” *Id.* at 1064. The Third Circuit found this declaration insufficient. The court was influenced in part by the staleness of the information, which stemmed from the 1930s. *Id.* But the court’s primary concern was that the FBI relied on speculation, rather than evidence. *Id.* “[I]f the government submits evidence that specific documents it has withheld contain secret information about techniques for recruiting informants,” *Davin* held, “it will have to establish that the release of this information would risk circumvention of the law. The speculation provided in the government’s brief of political groups’ increased ability to detect informants within their ranks is not supported by evidence.” *Id.*

Other courts, like *Davin*, consistently require the government to provide non-conclusory reasons why disclosure risks circumvention. *See, e.g., PHE, Inc. v. Dep’t of Justice*, 983 F.2d 248, 252 (D.C. Cir. 1993) (to meet its burden under Exemption 7(E), agency must “provid[e] reasons why releasing each [document] would create a risk of circumvention of the law”); *Voinche v. FBI*, 412 F. Supp. 2d 60, 69 (D.D.C. 2006) (FBI declaration that “merely quotes the statutory language of Exemption 7(E), and states: ‘[t]his existence of this procedure is not generally known to the public and the release of such may risk circumvention of the law’”

held insufficient to support exemption); *Feshbach v. SEC*, 5 F. Supp. 2d 774, 786-87 (N.D. Cal. 1997) (granting summary judgment for Plaintiffs because agency failed to “provide non-conclusory reasons why disclosure of” “internal procedures, techniques, and strategies” “would risk circumvention of the law”).

This Court’s decision in *Bowen v. FDA*, 925 F.2d 1225 (9th Cir. 1991), is not to the contrary. It held that “a detailed, technical analysis of the techniques and procedures used to conduct law enforcement investigations of product tamperings” was exempt, even though some information about cyanide-tracing techniques was already public. *Id.* at 1228-29. It did so however *because* the government’s affidavit “provide[d] detailed assertions” explaining how disclosure of the requested information would risk circumvention. *Id.* at 1229.

Citing Second Circuit precedent, the government asserts that 7(E)’s “risk of circumvention” requirement applies only to “guidelines” but not “techniques and procedures.” AOB at 35 n.10.¹⁵ But this Court in *Bowen*, as noted above, applied a risk of circumvention analysis to “techniques.” 925 F.2d at 1229. Other courts have done the same. *See, e.g., Blackwell v. FBI*, 646 F.3d 37, 42 (D.C. Cir. 2011) (finding information about techniques properly withheld because FBI

¹⁵ Exemption 7(E) allows the government to withhold records that “would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law.” 5 U.S.C. § 552(b)(7)(E).

demonstrated risk of circumvention); *Davin*, 60 F.3d at 1064 (requiring agency “to establish that the release of this information would risk circumvention of the law” to withhold “information about techniques for recruiting informants”); *Jones v. FBI*, 41 F.3d 238, 249 (6th Cir. 1994) (finding information about investigative techniques properly withheld because of risk of circumvention).

Requiring the government to prove risk of circumvention for techniques is also consistent with this Court’s precedent in *Rosenfeld*, which requires disclosure of techniques “generally known to the public,” 57 F.3d at 815, and thus rejected the “categorical protection” for techniques urged by the government here. AOB at 35 n.10. Conceptually, the “generally known” and “risk of circumvention” analyses are intertwined; disclosure of a technique that is generally known does not risk circumvention. As a result, “[i]t would not serve the purposes of FOIA . . . to keep secret an investigative technique that” does not risk circumvention. *See Rosenfeld*, 57 F.3d at 815; *see also Weiner*, 943 F.2d at 977 (agency must provide “a particularized explanation of how disclosure of the particular document would damage the interest protected by the claimed exemption”). Moreover, the government’s reading of the statute violates the principle that FOIA’s exemptions must be “narrowly construed” in favor of disclosure. *Kamman*, 56 F.3d at 48.

Contrary to the government’s assertion, the district court did not create a “categorical” rule that Exemption 7(E) is unavailable whenever information about

a technique enters the public domain. *See* AOB at 38. The district court correctly found that the public generally knows that the government can track location through cellular phones and vehicles, and that DOJ had not met its burden to explain why, under these circumstances, disclosure still risks circumvention. ER 23-25. Indeed, it is the government that seeks to create a *per se* rule that whenever an agency states that the “details” or “circumstances” of a technique’s use are unknown, all information about the technique is automatically exempt, even if the agency has not explained why disclosure risks circumvention. This position finds no support in the caselaw or the principles underlying FOIA.¹⁶

Finally, courts have affirmatively recognized that disclosure of legal standards does not give rise to a risk of circumvention. In *PHE*, the D.C. Circuit distinguished between a portion of an *investigatory* manual – which discussed,

¹⁶ Consistent with *Davin* and *Bowen*, the cases cited by DOJ, *see* AOB at 40, authorize an agency to withhold details of a technique if disclosure of the particular information would risk circumvention. *See Hale v. United States Dep’t of Justice*, 973 F.2d 894, 903 (10th Cir. 1992) (finding “techniques and procedures” protected because they “could reasonably be expected to risk circumvention of the law”) (emphasis added), *cert. granted, vacated and remanded on other grounds*, 509 U.S. 918 (1993); *Barnard v. Dep’t of Homeland Security*, 598 F. Supp. 2d 1, 23 (D.D.C. 2009) (“Defendant’s description of the withheld information and the reasons why disclosure would allow circumvention of the law are sufficiently descriptive.”); *Asian Law Caucus v. United States Dep’t of Homeland Security*, No. 08-00842, 2008 WL 5047839, at *5 (N.D. Cal. Nov. 24, 2008) (not deciding whether government required to prove risk of circumvention for techniques, but concluding after *in camera* review that information protected under 7(E) because disclosure “could reasonably be expected to risk circumvention”).

among other things, ““sources of information available to Agents investigating obscenity violations”” – and a *legal* manual that provided ““a step by step analysis of [obscenity] law.”” 983 F.2d at 251. Disclosure of the former risked circumvention because potential violators could “tamper” with “sources of information” identified in the document. *Id.* But disclosure of the legal manual’s discussion of the law “is precisely the type of information appropriate for release under the FOIA,” which “mandates the release of materials that contain ‘secret law.’” *Id.* Indeed, disclosure of the legal standards applied by the government “could lead to compliance with, rather than risk circumvention of, the law.” *Id.* at 252; *see also Hawkes v. IRS*, 507 F.2d 481, 484 (6th Cir. 1974) (“[D]isclosure of information clarifying an agency’s substantive or procedural law serves the very goals of enforcement by encouraging knowledgeable and voluntary compliance with the law.”). The D.C. Circuit thus found the agency not to have met its burden under Exemption 7(E). *PHE*, 983 F.2d at 251-52.

B. DOJ Failed to Meet its Burden of Demonstrating a Risk of Circumvention

The government has not met its burden of explaining why disclosure of the “circumstances” in which the government uses commonly known location tracking technologies would create a risk of circumvention. Indeed, it cannot meet that burden because these documents address the legal standards used by the

government when deploying these technologies. That is not the type of information Exemption 7(E) protects from disclosure.

DOJ's initial declaration stated that the techniques discussed in CRM Four and Five "are not publicly known." ER 46. Plaintiffs submitted evidence, however, showing that bald assertion to be false.

CRM Four discusses a number of techniques – all various forms of tracking someone's location through their cellular phone or vehicle: "Obtaining Location Information from Wireless Carriers," "Mobile Tracking Devices," and "Telematics Providers (OnStar, etc.)." ER 50. CRM Five describes "electronic tracking devices – generally and cellular telephone location information." *Id.* at 57. The government's technique of obtaining location information from wireless carriers is already well known, as evidenced by extensive media coverage. *See* SER 68-71. Also well known to the public is the government's use of "mobile tracking devices," such as GPS and cell site simulators (also called stingrays, digital analyzers, or triggerfish), which are discussed in DOJ's own publications and have been the subject of extensive media coverage. *See* SER 68-69, 115, 132, 179-232. Finally, the public is already well aware that the government can obtain location information from telematics providers such as OnStar. *See* SER 172-77. The record is clear that the location tracking methods discussed in CRM Four and Five

are “commonly known techniques.” *See* S. Rep. No. 93-1200 (1974) (Conf. Rep.), *reprinted in* 1974 U.S.C.C.A.N. 6285, 6291.

On reply, the agency retreated somewhat, admitting that “the public may know that federal investigators use some of these techniques,” but asserting that “the details of their use are not publicly known. CRM Four and Five discuss such non-public details as where, when, how, and under what circumstances electronic surveillance, tracking devices and non-wiretap electronic surveillance investigative techniques are used.” ER 34-35.

Although the facts of *Rosenfeld* are not directly analogous – CRM Four and Five do not discuss the application of well-known techniques in specific cases – its reasoning applies here. DOJ initially stated that the techniques are not publicly known. But when faced with overwhelming contrary evidence, it recharacterized the information sought as pertaining not just to the technique but “details of their use.” ER 34. This Court in *Rosenfeld* recognized that such slippery characterizations of the technique would invite abuse. The government should not be permitted to avoid disclosure of even well known techniques “simply by saying that the ‘investigative technique’ at issue is not the practice but” details about the practice. 57 F.3d at 815; *see also Davin*, 60 F.3d at 1049 (“The review of FOIA cases is made difficult by the fact that the party seeking disclosure does not know the contents of the information sought and is, therefore, helpless to contradict the

government's description of the information or effectively assist the trial judge.") (internal quotation marks, citation omitted).

Nor can the government rest on the unelaborated assertion that CRM Four and Five address the "circumstances" in which location tracking technologies are used. It must still explain why disclosure risks circumvention. *See Davin*, 60 F.3d at 1064 (finding insufficient declaration stating that documents discussed "the manner in which informants are identified, recruited, cultivated and handled by the FBI").

The district court correctly held that the government failed to do so. As the court below observed, the public is well aware that the government tracks location through cellular phones and vehicles; potential violators already know that to evade detection, they need only limit phone and vehicle usage. ER 24. And while DOJ states that the documents describe the "circumstances" under which these technologies are deployed, it fails to describe the "circumstances" with sufficient specificity to allow a meaningful assessment of whether disclosure would risk circumvention. *See Weiner*, 943 F.2d at 977 (agency's declaration must provide sufficiently particularized information "to afford the FOIA requester a meaningful opportunity to contest, and the district court an adequate foundation to review, the soundness of the withholding").

The government's vague declaration does not meet its burden because there are several ways in which disclosure of the "circumstances" of a technology's use would *not* risk circumvention. For example, documents that address the "circumstances" under which location tracking technologies are used might discuss the types of crimes for which the techniques are employed, perhaps, kidnapping and drug conspiracies. But the only way this information could assist potential violators in avoiding the government's location tracking efforts is if they refrained from committing those crimes. *See PHE*, 983 F.2d at 252 (disclosure of government's legal standards "could lead to compliance with, rather than risk circumvention of, the law"). Disclosure of information of this sort "serves the very goals of enforcement by encouraging knowledgeable and voluntary compliance with the law." *Hawkes*, 507 F.2d at 484. To the extent DOJ hypothesizes that a potential kidnapper, if given this information, would choose instead to commit a different crime, it must offer "evidence" and not "speculation." *Davin*, 60 F.3d at 1064.

Another (not mutually exclusive) possibility, and one consistent with the record, is that the documents set forth the types of legal safeguards used by the government before deploying various kinds of location tracking technology. For example, does the government use a particular location tracking technology after obtaining a Pen Register order, which requires only a showing of "relevance," 18

U.S.C. § 3123(d), or after obtaining a warrant based on a higher showing of probable cause? But the only way this information could risk circumvention is if potential law violators refrained from conduct that satisfied the legal threshold (by, for example, deciding to stop violating the law). The government's declarations nowhere explain how information about legal standards risks circumvention.

“Material like this is precisely the type of information appropriate for release under the FOIA” because it constitutes “secret law.” *PHE*, 983 F.2d at 251-52; *see supra* Part I-C.

A third possibility is that the documents contain technical information about how the surveillance is implemented. For example, they might explain that FBI agents typically place GPS devices in the air filter compartment of an engine because people rarely look there. But if that is actually the type of information contained in these documents, it would have been easy enough for the government to have explained, without compromising the information it sought to withhold, that the documents identify where tracking devices are placed. Unlike the agency in *Bowen*, DOJ failed to provide “detailed assertions” that CRM Four and Five contain a “detailed, technical analysis” of location tracking technologies, disclosure of which risks circumvention. 925 F.2d at 1228-29. Instead, the government here relies on the conclusory assertion that the documents discuss some unspecified set of “circumstances” in which the technologies are used and

from which it does not necessarily follow that disclosure would risk circumvention.

To be sure, the government may articulate on reply another theory as to why disclosure of the “circumstances” or “details” of the technology’s use risks circumvention. But it cannot make up in its brief what its declaration lacks in specificity.

DOJ contends that a number of courts have protected from disclosure “the kinds of details at issue here.” AOB at 40. But unlike DOJ, the agencies in these other cases did not rely on broad assertions that the documents discussed unspecified “details” about a technique. Rather, they provided a sufficient description of the type of details at issue to permit an assessment of whether disclosure would risk circumvention. *See Miller v. United States Dep’t of Justice*, 562 F. Supp. 2d 82, 124 (D.D.C. 2008) (“exact nature and type of information used to develop” “criminals’ psychological profiles”); *Brunetti v. FBI*, 357 F. Supp. 2d 97, 108 (D.D.C. 2004) (section of investigative form used by law enforcement agents to make notations about the most useful investigative techniques); *Maguire v. Mawn*, No. 02 Civ. 2164, 2004 WL 1124673, at *2 (S.D.N.Y. May 19, 2004) (whether particular bank used bait money); *Wickline v. FBI*, No. 92-1189, 1994 WL 549756, at *5 (D.D.C. Sept. 30, 1994) (disclosure of specific manner in which recording equipment was used in a particular case “would allow individuals to

develop ‘conversations to mislead the FBI’”). Here, the government has simply failed to say what types of details these documents contain.¹⁷

Moreover, even if the government had provided sufficiently specific information in its declaration to justify withholding some information, it has failed to demonstrate that it released all reasonably segregable information. *See* 5 U.S.C. § 552(b) (requiring agencies to provide “[a]ny reasonably segregable portion of a record . . . after deletion of the portions which are exempt under this subsection”); *Mead Data Cent., Inc. v. United States Dep’t of the Air Force*, 566 F.2d 242, 261 (D.C. Cir. 1977) (agencies must “provide the reasons behind their conclusions” that a document is not reasonably segregable and “describe what proportion of the information in a document is non-exempt and how that material is dispersed throughout the document”).¹⁸

¹⁷ The government notes that the documents also reflect law enforcement “guidelines” and not only “techniques.” *See* AOB at 39 n. 11. But this adds nothing to the analysis. As DOJ concedes, the government must still prove risk of circumvention for guidelines.

¹⁸ DOJ’s declaration is indistinguishable from conclusory recitations of the legal standard courts have repeatedly found to “fall short of the specificity required . . . to properly determine whether the non-exempt information is, in fact, not reasonably segregable.” *Compare, e.g., Branch v. FBI*, 658 F. Supp. 204, 210 (D.D.C. 1987) (FBI affidavit stated “[e]very effort was made to provide plaintiff with all reasonably segregable non-exempt portions of the material requested”), *with* ER 47 (“The documents withheld in their entirety contain no meaningful portion that could be released without destroying the integrity of the document.”).

In short, the mere assertion without more that the documents identify the manner in which location tracking technologies are used does not suffice to carry the government's burden. *See Davin*, 60 F.3d at 1064. Indeed, because the documents pertain to the legal standards used by the government before deploying the technology, they constitute "secret law" and are "precisely the type of information appropriate for release under the FOIA." *PHE*, 983 F.2d at 251-52.

C. The Agency Is not Entitled to a Second Chance to Meet its Burden

The government contends that "if there were any doubt" about whether it met its burden, the court below should have conducted an *in camera* review or given the agency an opportunity to submit additional declarations. AOB at 34; *see also id.* at 43 n.12.

The agency bears the burden in a FOIA action. *See Kamman*, 56 F.3d at 48. The court ruled on cross-motions for partial summary judgment. ER 1. When a party in a summary-judgment motion "fails to properly support an assertion of fact," Federal Rule of Civil Procedure 56 expressly gives the district court the discretion either to give that party "an opportunity to properly support" that fact or instead to simply "grant summary judgment if the motion and supporting materials . . . show the movant is entitled to it." Fed. R. Civ. P. 56(e)(1), (3).

The agency, unlike Plaintiffs, had "unilateral and uninhibited access to the content of the withheld documents," *State of Maine v. United States Dep't of*

Interior, 298 F.3d 60, 73 (1st Cir. 2002), and every opportunity to develop the record. It submitted two declarations with its opening brief, a supplemental declaration with its reply, and stood on the adequacy of the record it submitted below. *See* ER 96-97 (Docket Entries 23 and 33); SER 55 (“The Declarations provide ample evidence that establishes the need for an exemption.”). The district court “did not abuse its discretion in denying the agency ‘a second chance.’” *State of Maine*, 298 F.3d at 73 (rejecting agency’s contention in FOIA action that district court should have granted it “opportunity to submit additional affidavits” instead of ordering disclosure); *see also Coastal States*, 617 F.2d at 870 (affirming district court’s disclosure order where agency failed to carry its burden).

Allowing the government to submit more declarations would simply encourage delay: agencies could submit inadequate declarations without consequence, endlessly staving off disclosure. Such an outcome would undermine FOIA’s efficacy, *see* H.R. Rep. No. 93-876 (1974), *reprinted in* 1974 U.S.C.C.A.N. 6267, 6271 (Congressional recognition that delay in complying with FOIA requests may be “tantamount to denial”), and would be particularly inappropriate here, where Plaintiffs sought and the agency granted expedited processing on a request originally submitted in 2012. ER 75, 90.

Nor did the district court err in declining to conduct an *in camera* review. *See Church of Scientology*, 611 F.2d at 743 (“[T]he burden of proof in FOIA cases

remains squarely on the government, and . . . [i]n camera inspection is a procedure which the trial court need invoke only where it finds inspection appropriate, in its discretion.”). Plaintiffs, however, have no objection to *in camera* review by this Court.

CONCLUSION

For the foregoing reasons, the decision below should be affirmed.

DATED: June 22, 2015

Respectfully submitted,

By: /s/ Linda Lye
Linda Lye

LINDA LYE (SBN 215584)
llye@aclunc.org
MICHAEL T. RISHER (SBN 191627)
mrisher@aclunc.org
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF NORTHERN
CALIFORNIA, INC.
39 Drumm Street
San Francisco, CA 94111
Telephone: (415) 621-2493
Facsimile: (415) 255-8437

Attorneys for Plaintiffs-Appellees

**CERTIFICATE OF COMPLIANCE WITH FEDERAL RULE OF
APPELLATE PROCEDURE 32(a)**

I hereby certify that Plaintiffs-Appellees' Answering Brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because it contains 13,514 words, excluding the parts of the brief exempted by Fed. R. App. P.

32(a)(7)(B)(iii). I hereby further certify that this brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and (6) because it has been prepared in 14-point Times New Roman, a proportionally spaced font.

DATED: June 22, 2015

By: /s/ Linda Lye
Linda Lye

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing Answering Brief for Plaintiffs-Appellees with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system on June 22, 2015. I further certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

DATED: June 22, 2015

By: /s/ Linda Lye
Linda Lye

STATEMENT OF RELATED CASES

Plaintiffs-Appellees are not aware of any cases in this Court that are deemed related within the meaning of this Court's Rule 28-2.6.

DATED: June 22, 2015

By: /s/ Linda Lye
Linda Lye

From: Winn, Peter A. (OPCL)
Subject: Draft Annual Report
To: Brown Lee, Erika (ODAG)
Cc: Mayer, Hannah J. (OPCL); Proia, Andrew (OPCL); Young, Brian A. (OPCL); Barnes, Khaliah N (JMD); Zelman, Beth (OPCL)
Sent: December 9, 2016 4:26 PM (UTC-05:00)
Attached: AnnualPrivacyReport Dec 9 Draft.docx

Hi Erika,

Here is a copy of the Annual Report for your review. As I mentioned, we are still double checking the numbers and still need to coordinate with some of the components to make sure some of the information may be released to the public. Also the outreach portion of the document is incomplete, and still needs to be supplemented with the CPCLO's and the Director's outreach activities (I'm also need to circle back with Kristi on her activities).

Subject to that, however, this document should be ready for your review.

Peter A. Winn
Director, Office of Privacy and Civil Liberties
United States Department of Justice
National Place Building, Suite 1000
1331 Pennsylvania Avenue, NW
Washington DC 20530
Office (b) (6)
Cell (b) (6)
Fax (202) 307-0693
(b) (6)

From: Young, Brian A. (OPCL)
Subject: RE: Oversight & Government Reform Committee Report---Law Enforcement Use of Cell-Site Simulation Technologies: Privacy Concerns and Recommendations
To: Proia, Andrew (OPCL)
Sent: December 19, 2016 1:01 PM (UTC-05:00)
Thanks Andrew.

I'm sure we'll be hearing more about this.

Brian A. Young
Senior Counsel
Office of Privacy and Civil Liberties (OPCL)
U.S. Department of Justice

(b) (6) (office)

(b) (6) (mobile)

(202) 307-0693 (fax)

SECRET: (b) (6)

TS: (b) (6)

NOTICE: This email (including any attachments) is intended for the use of the individual or entity to which it is addressed. It may contain information that is privileged, confidential, or otherwise protected by applicable law. If you are not the intended recipient (or the recipient's agent), you are hereby notified that any dissemination, distribution, copying, or use of this email or its contents is strictly prohibited. If you received this email in error, please notify the sender immediately and destroy all copies.

From: Proia, Andrew (OPCL)
Sent: Monday, December 19, 2016 12:55 PM
To: Brown Lee, Erika (ODAG); Winn, Peter A. (OPCL); Young, Brian A. (OPCL); Barnes, Khaliah N (JMD); Mayer, Hannah J. (OPCL); Zelman, Beth (OPCL)
Subject: Oversight & Government Reform Committee Report---Law Enforcement Use of Cell-Site Simulation Technologies: Privacy Concerns and Recommendations

All,

For your situational awareness:

Committee on Oversight and Government Reform U.S. House of Representatives 114th Congress, Bipartisan Report, *Law Enforcement Use of Cell-Site Simulation Technologies: Privacy Concerns and Recommendations* <https://oversight.house.gov/wp-content/uploads/2016/12/THE-FINAL-bipartisan-cell-site-simulator-report.pdf>

House Oversight and Government Reform Committee Chairman Jason Chaffetz (R-UT) and Ranking Member Elijah Cummings (D-MD) released a bipartisan staff report after a yearlong

investigation into federal, state, and local law enforcement use of cell-site simulators – devices that transform a cell phone into a real-time tracking device.

The report finds these law enforcement agencies have varying policies for the use of these powerful devices. As a result, the report recommends Congress pass legislation to establish a clear, nationwide framework that ensures the privacy of all Americans are adequately protected. <https://oversight.house.gov/report/bipartisan-committee-staff-report-clear-guidelines-needed-stingray-devices/>

Regards,

Andrew A. Proia
Attorney Advisor
U.S. Department of Justice
Office of Privacy and Civil Liberties (OPCL)
National Place Building, Suite 1000
1331 Pennsylvania Avenue NW
Washington, DC 20530
(b) (6) (office)
(b) (6) (mobile)
(202) 307-0693 (fax)
(b) (6)

NOTICE: This email (including any attachments) is intended for the use of the individual or entity to which it is addressed. It may contain information that is privileged, confidential, or otherwise protected by applicable law. If you are not the intended recipient (or the recipient's agent), you are hereby notified that any dissemination, distribution, copying, or use of this email or its contents is strictly prohibited. If you received this email in error, please notify the sender immediately and destroy all copies.

From: Brown Lee, Erika (ODAG)
Subject: Annual Report
To: Winn, Peter A. (OPCL); Proia, Andrew (OPCL) ((b) (6))
Sent: December 28, 2016 6:13 PM (UTC-05:00)
Attached: AnnualPrivacyReport Dec 9 Draft- EBL Edits.docx

Hi Peter – thanks again to Team OPCL for putting together a very impressive document. Attached are my edits. Please note that I reorganized the text referring to our international efforts into a separate section in order to capture our extensive efforts on that front.

Best regards,
Erika

Erika Brown Lee
Chief Privacy and Civil Liberties Officer
Office of the Deputy Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, D.C. 20530
Tel: (b) (6)
(b) (6)
TS: (b) (6)

From: Brown Lee, Erika (ODAG)
Subject: RE: Annual Report
To: Winn, Peter A. (OPCL); Proia, Andrew (OPCL) ((b) (6))
Sent: December 28, 2016 6:34 PM (UTC-05:00)
Attached: AnnualPrivacyReport Dec 9 Draft- EBL Edits.docx

Please use this version as I'm not sure the version I sent earlier captures all the edits.

Erika Brown Lee
Chief Privacy and Civil Liberties Officer

Office of the Deputy Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, D.C. 20530

Tel: (b) (6)

(b) (6)

TS: (b) (6)

From: Winn, Peter A. (OPCL)
Sent: Wednesday, December 28, 2016 6:24 PM
To: Brown Lee, Erika (ODAG) <(b) (6)>
Cc: Proia, Andrew (OPCL) <(b) (6)>
Subject: Re: Annual Report

Got it.

On Dec 28, 2016, at 3:17 PM, Brown Lee, Erika (ODAG) <(b) (6)> wrote:

Pushed send too soon. On the outreach section, Andrew's panel on CISA, and Jenny's meeting with advocates for the Open Gov initiative should be included.

Thanks,
Erika

Erika Brown Lee
Chief Privacy and Civil Liberties Officer

Office of the Deputy Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, D.C. 20530

Tel: (b) (6)

(b) (6)

TS: (b) (6)

From: Brown Lee, Erika (ODAG)
Sent: Wednesday, December 28, 2016 6:13 PM
To: Winn, Peter A. (OPCL) <(b) (6)>; Proia, Andrew (OPCL) ((b) (6))
<(b) (6)>
Subject: Annual Report

Duplicative Information - See Document ID 0.7.12327.13515

From: Mayer, Hannah J. (OPCL)
Subject: Annual Report Final Draft
To: Brown Lee, Erika (ODAG); Winn, Peter A. (OPCL)
Cc: Proia, Andrew (OPCL)
Sent: January 4, 2017 2:22 PM (UTC-05:00)
Attached: AnnualPrivacyReport_FINAL(draft).docx

Dear Erika and Peter,

Please find attached the Annual Report final draft that is ready to be sent to components for comment. Once you clear that this draft may be sent, I will send to Rana at OLA.

After speaking with Rana, she informed me that the entire clearance process should take about **two weeks**.

If I send the draft to Rana **today**, she will circulate to the components before **COB** with a comment period until **Monday, December 9, 2017**. Then, OPCL will receive the internal component comments back that **Monday**. Once we review the internal comments, then the draft will go to ODAG to be cleared, which should take about **two days** for ODAG to clear. Once ODAG clears the document, the draft will be sent to OMB for clearance.

Please let me know if you have any questions.

Thank you,

Hannah

Hannah Mayer
Attorney Advisor
Office of Privacy and Civil Liberties
U.S. Department of Justice
National Place Building, Suite 1000
1331 Pennsylvania Avenue, NW
Washington, DC 20530

(b) (6) (office)

(b) (6) (cell)

202.307.0693 (fax)

(b) (6)

From: Mayer, Hannah J. (OPCL)
Subject: OPCL Annual Report
To: Wahdan, Rana S. (OLA)
Cc: Brown Lee, Erika (ODAG); Winn, Peter A. (OPCL); Proia, Andrew (OPCL)
Sent: January 4, 2017 4:07 PM (UTC-05:00)
Attached: AnnualPrivacyReport_FINAL(draft).docx

Dear Rana,

Please find attached OPCL's Annual Report for component comments. Please let me know if you need anything else.

Thank you for your assistance.

Best,

Hannah

Hannah Mayer
Attorney Advisor
Office of Privacy and Civil Liberties
U.S. Department of Justice
National Place Building, Suite 1000
1331 Pennsylvania Avenue, NW
Washington, DC 20530

(b) (6) (office)

(b) (6) (cell)

202.307.0693 (fax)

(b) (6)

From: Brown Lee, Erika (ODAG)
Subject: Quote for DAG
To: Winn, Peter A. (OPCL)
Sent: January 4, 2017 4:45 PM (UTC-05:00)

At the Department of Justice, we have always viewed the principles of privacy and civil liberties as fundamental to our mission to ensure the fair and impartial administration of justice. DOJ's Privacy Forum serves as an important platform in strengthening relationships across the Department while engaging in a discussion of current privacy-related topics. Examples of the impact of privacy on the Department's activities include our recently issued policies on the emerging technologies of unmanned aircraft systems and cell-site simulators. Consistent with our efforts as a trusted partner with the American public, we continue to value increased transparency and enhanced security regarding the data we entrusted to our care.

Erika Brown Lee
Chief Privacy and Civil Liberties Officer
Office of the Deputy Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, D.C. 20530
Tel: (b) (6)
(b) (6)
TS: (b) (6)