RSAConference2018
San Francisco | April 16–20 | Moscone Center

SESSION ID: PRV-T08

NOBODY PUTS PRIVACY IN A CORNER: PRIVACY IN ENTERPRISE RISK MANAGEMENT

Jamie Danker

Director, Senior Privacy Officer
National Protection and Programs Directorate, U.S. Department of Homeland Security (DHS)

Naomi Lefkovitz

Senior Privacy Policy Advisor
National Institute of Standards and Technology (NIST)

NIST Guidance

- **NIST Internal Report (NISTIR) 8062:** *An Introduction to Privacy Engineering and Risk Management in Federal Systems*
- **NIST Special Publication (SP) 800-37 (rev. 2 draft):** *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*
- **NIST SP 800-53 (rev. 5 draft):** *Security and Privacy Controls for Information Systems and Organizations*

DHS Automated Indicator Sharing

- Cybersecurity Act of 2015, Title I “Cybersecurity Information Sharing Act (CISA)”
  - Designates DHS as the central hub for the sharing of cyber threat indicators between the private sector and the Federal Government
- DHS Automated Indicator Sharing (AIS) capability enables the exchange of cyber threat indicators between the Federal Government and the private sector at machine speed.
- Key Design Objective: Engender trust amongst participants by sharing cyber threat indicators and defensive measures that are directly related to cyber threats in real-time while protecting privacy and civil liberties.

GETTING AROUND THE TOP 7 PRIVACY MISCONCEPTIONS AND MISTAKES THAT IMPEDE ENTERPRISE RISK MANAGEMENT

#1: SECURITY AND PRIVACY CONFLATION

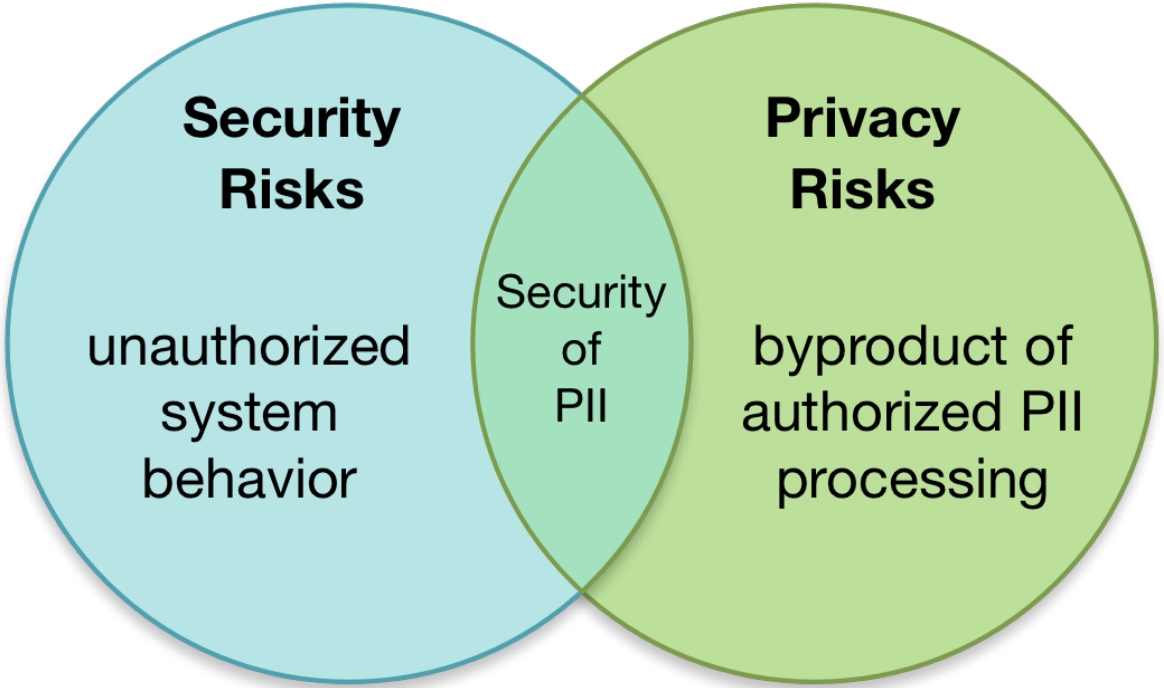
Security and Privacy Conflation

We have security safeguards in place, so we have privacy covered.

CONFIDENTIALITY  PRIVACY

Security and Privacy Conflation

NISTIR 8062



Security and Privacy Conflation

Security Risk Model

Factors:

Likelihood | Threats | Vulnerabilities | Impact

Privacy Risk Model

Factors:

Likelihood | **Problematic Data Action** | Impact

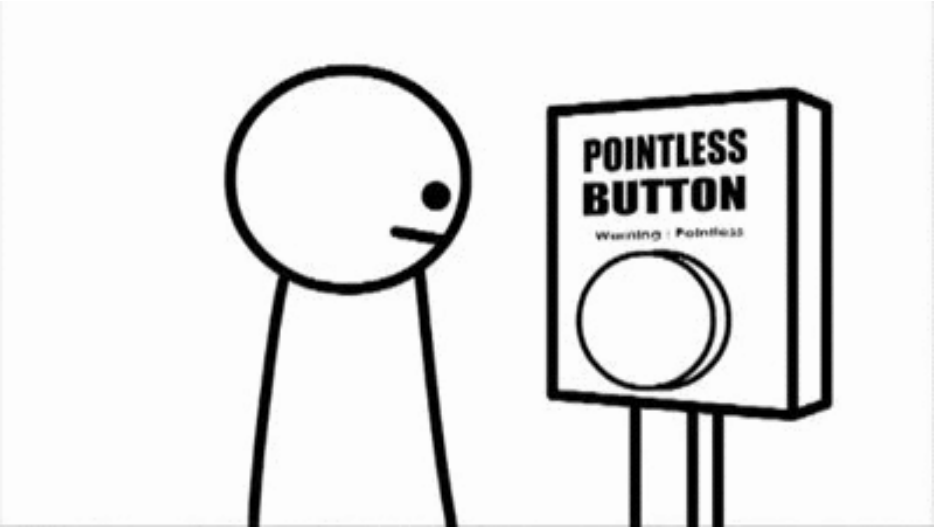
Problematic Data Action

a data action that causes an adverse effect, or problem, for individuals

#2: PRIVACY IS DEAD

Privacy Is Dead

Why bother? Everyone's data is already out there.



http://gifimage.net/wp-content/uploads/2017/01/ASDF-GIF-Image-for-Whatsapp-and-Facebook-47.gif

#3: THE TRAIN HAS LEFT THE STATION

The Train Has Left the Station

The system has already been deployed – it's too late to think about privacy.

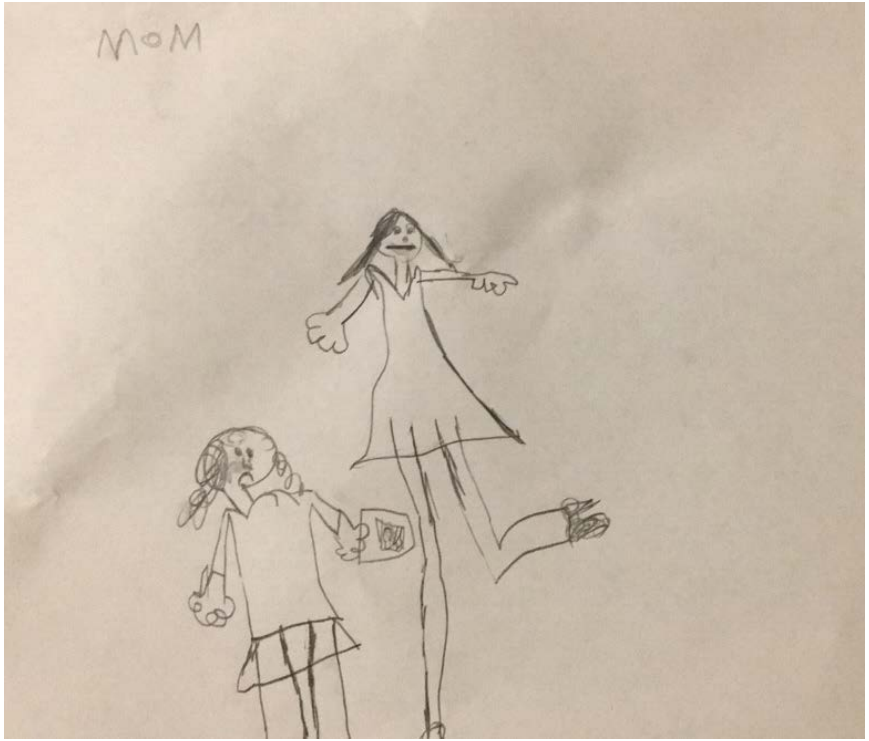
https://thumbs.gfycat.com/TenseTenderHart-size_restricted.gif

#4: PRIVACY KISS OF DEATH (FUN FUN FUN ’TIL PRIVACY TAKES THE T-BIRD AWAY)

Privacy Kiss of Death

"Privacy is a wet blanket that ruins all the fun."

"We won't be able to set up the system that we want if we think about privacy."



#5: PRIVACY WINDEX

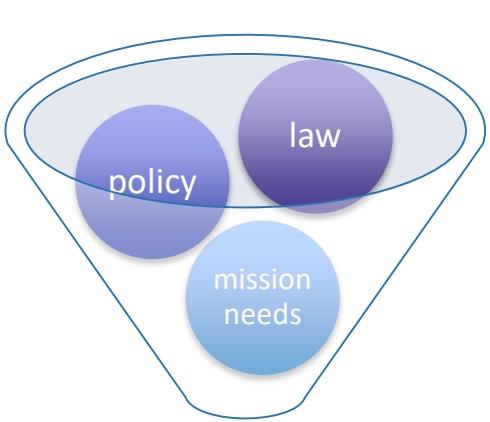
Privacy Windex

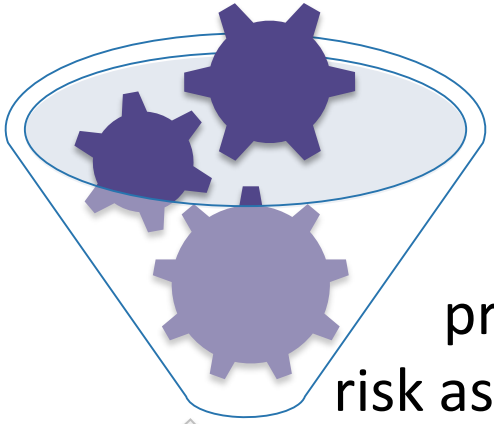
Privacy is just legal compliance. All we need to do is spray legal compliance all over the system, and then we're all good on privacy.

http://www.theluxuryspot.com/wp-content/uploads/2014/05/tumblr_ma0zg9vAyI1qakgc1o1_500.gif

Privacy Windex

Legal compliance is a piece of the whole privacy pie.





privacy risk assessment

System Privacy Requirements

#6: DATA HOARDING

Data Hoarding

We need to collect as much data as possible - we might need it later!

https://img.buzzfeed.com/buzzfeed-static/static/2015-02/26/14/enhanced/webdr12/anigif_enhanced-19706-1424977768-34.gif?downsize=715:*&output-format=auto&output-quality=auto

SP 800-53 (rev 4) App J: DM-1 Minimization of Personally Identifiable Information

- The organization:
  - a. Identifies the minimum personally identifiable information (PII) elements that are relevant and necessary to accomplish the legally authorized purpose of collection;
  - b. Limits the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent; and
  - c. Conducts an initial evaluation of PII holdings and establishes and follows a schedule for regularly reviewing those holdings [Assignment: organization-defined frequency, at least annually] to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose.

Proposed Rev 5: Data Minimization

Reframing data minimization to align with a risk-based approach for more effective privacy protections

Examples:

- **SI-12(1) Information Management And Retention | Limit Personally Identifiable Information Elements**

Limit personally identifiable information being processed in the information life cycle to the [Assignment: organization-defined elements] identified in the privacy risk assessment

- **SC-42(5) Sensor Capability and Data | Collection Minimization**

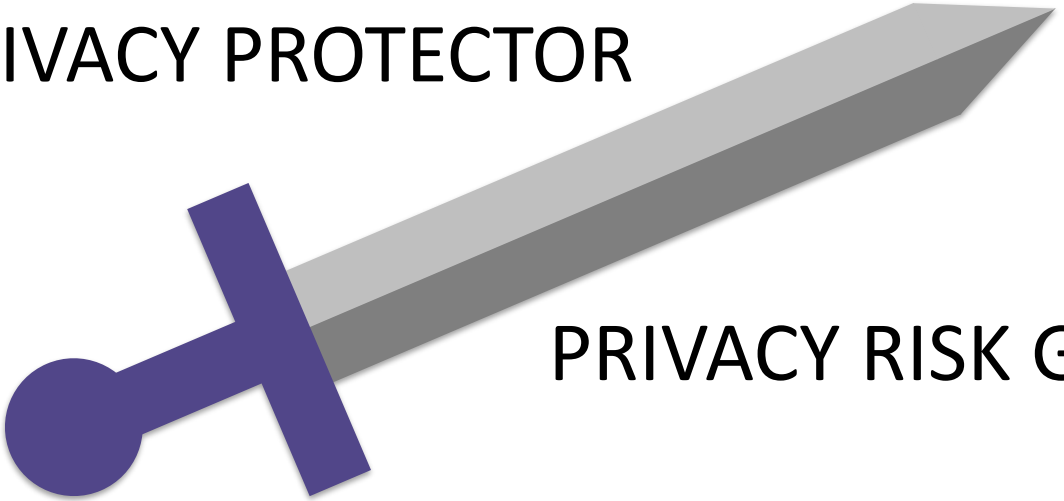
Employ [Assignment: organization-defined sensors] that are configured to minimize the collection of information about individuals that is not needed.

#7: THE DOUBLE EDGED SWORD

The Double Edged Sword

All our security safeguards are awesome and have no impact on privacy.

PRIVACY PROTECTOR



PRIVACY RISK GENERATOR

The Double Edged Sword

Digital identity is a prime example of the Double Edged-Sword…

"Digital authentication supports privacy protection by mitigating risks of unauthorized access to individuals' information. At the same time, because identity proofing, authentication, authorization, and federation involve the processing of individuals' information, these functions can also create privacy risks. These guidelines therefore include privacy requirements and considerations to help mitigate potential associated privacy risks."

NIST SP 800-63

Resources

Don’t fall victim to the 7 privacy misconceptions and mistakes!

- NISTIR 8062: https://doi.org/10.6028/NIST.IR.8062
- NIST SP 800-37 (revision 2 discussion draft): https://csrc.nist.gov/CSRC/media/Publications/sp/800-37/rev-2/draft/documents/sp800-37r2-discussion-draft.pdf
- NIST SP 800-53 (revision 5 DRAFT): https://csrc.nist.gov/CSRC/media//Publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf
- NIST SP 800-63: https://pages.nist.gov/800-63-3/
- DHS AIS: https://www.us-cert.gov/ais

Instructions to have the “Time of Your Life”

- Next week you should:
  - Review NIST guidance and seek out your organization’s privacy team.
- In the first three months following this presentation you should:
  - Be on the look out for where your organization has fallen victim to privacy misconceptions and mistakes in the past and create opportunities for an enterprise risk management process that considers privacy AND security.
- Within six months you should:
  - Identify the progress of security and privacy integration in your organization. and share lessons learned.

The Goal

The Goal


PRIVACY AND SECURITY
TOGETHER
NAILED IT!
memegenerator.net

Q&A