



The global voice of scholarly publishing

The User in User Privacy

An STM User Privacy WG Perspective

IJsbrand Jan Aalbersberg – Elsevier

STM US Annual Conference 2016

Washington - April 28, 2016

Contents

- Privacy – what is to be protected
- Personal data – what can it be used for
- The user – expectations and value
- How to build trust with the user?
- Responsibilities of the product team
- Helper guides and concepts

Diving into some details

- **Personal data**: Any information relating to an identified or identifiable natural person (EU)
- **Privacy**: The state or condition of being free from being observed or disturbed by other people (OD)
- **Data Privacy**: Informational privacy encompasses an individual's freedom from excessive intrusion ... and an individual's ability to choose ... which his or her beliefs, behaviors, opinions, and attitudes will be shared with or withheld from others. [National Research Council and the Social Science Research Council]

What is protected?

- **Personal data**: Any information relating to an identified or **identifiable** natural person (EU)
- **Privacy**: The state or condition of being free from being observed or disturbed by other people (OD)
- **Data Privacy**: Informational privacy encompasses an individual's freedom from excessive intrusion ... and an individual's ability to choose ... which his or her beliefs, behaviors, opinions, and attitudes will be shared with or withheld from others. [National Research Council and the Social Science Research Council]

What is protected?

- **Personal data**: **Any information** relating to an identified or identifiable natural person (EU)
- **Privacy**: The state or condition of being free from being observed or disturbed by other people (OD)
- **Data Privacy**: Informational privacy encompasses an individual's freedom from excessive intrusion ... and an individual's ability to choose ... which his or her beliefs, behaviors, opinions, and attitudes will be shared with or withheld from others. [National Research Council and the Social Science Research Council]

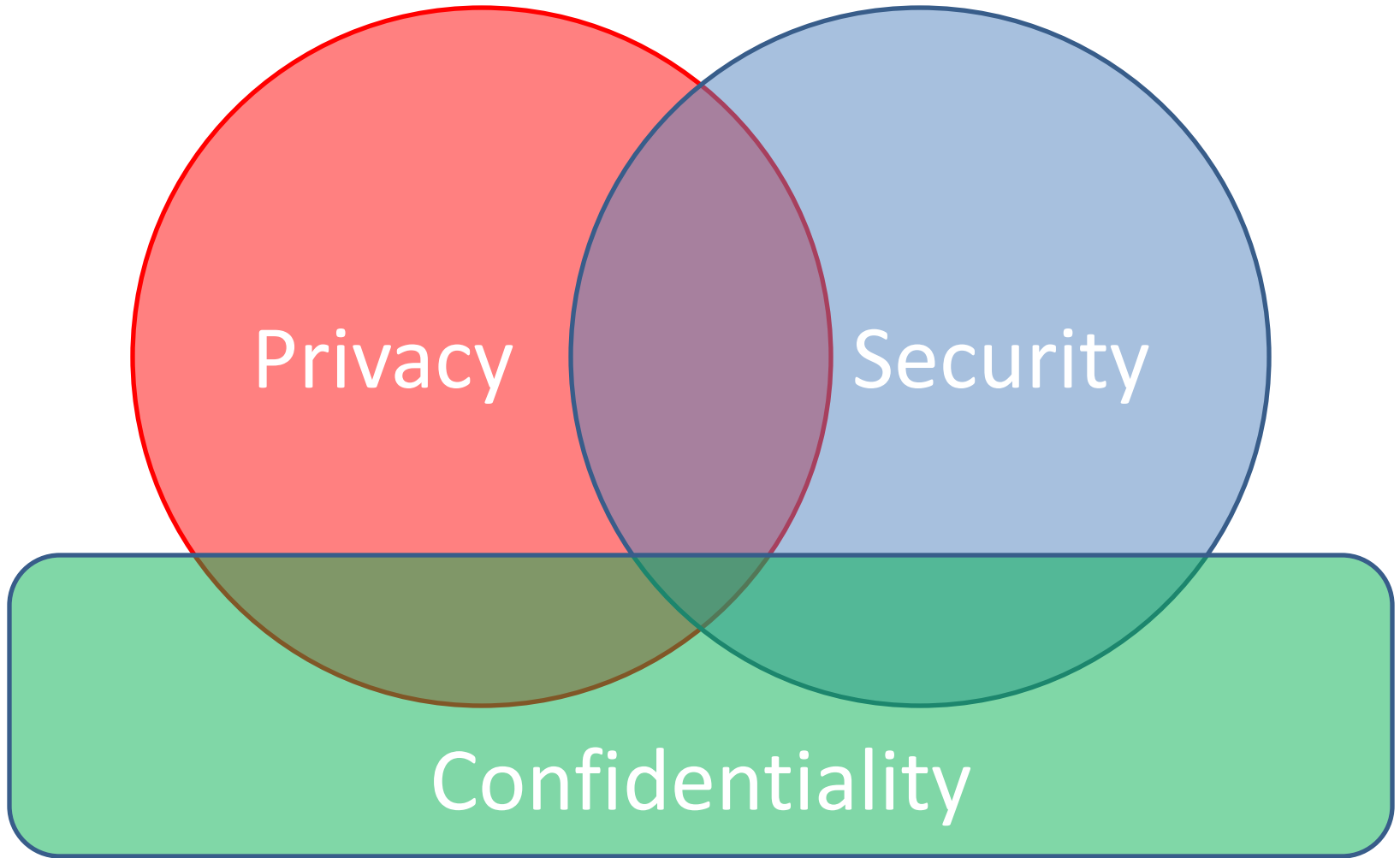
Protected against whom?

- **Personal data**: Any information relating to an identified or identifiable natural person (EU)
- **Privacy**: The state or condition of being free from being observed or disturbed by **other people** (OD)
- **Data Privacy**: Informational privacy encompasses an individual's freedom from excessive intrusion ... and an individual's ability to choose ... which his or her beliefs, behaviors, opinions, and attitudes will be shared with or withheld from others. [National Research Council and the Social Science Research Council]

Protected against what?

- **Personal data**: Any information relating to an identified or identifiable natural person (EU)
- **Privacy**: The state or condition of **being free** from being observed or disturbed by other people (OD)
- **Data Privacy**: Informational privacy encompasses an individual's freedom from excessive intrusion ... and an individual's ability to choose ... which his or her beliefs, behaviors, opinions, and attitudes will be shared with or withheld from others. [National Research Council and the Social Science Research Council]

Privacy <> Security



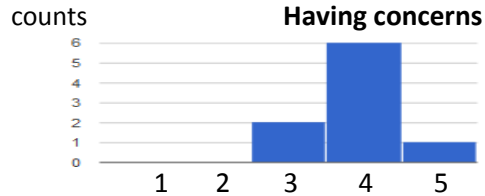
Not black and white

- Privacy: The state or condition of being free from being observed or disturbed by other people (OD)
- Personal data: Any information relating to an identified or identifiable natural person (EU)
- Data Privacy: Informational privacy encompasses an individual's freedom from **excessive intrusion** ... and an individual's ability to **choose** ... which his or her beliefs, behaviors, opinions, and attitudes will be **shared** with or withheld from others. [National Research Council and the Social Science Research Council]

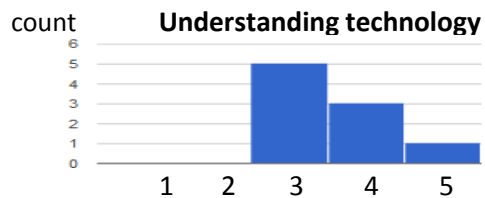
Wikipedia adds: expectation!

- Data privacy is the relationship between [WP]:
 - collection and dissemination of data,
 - technology,
 - **the public expectation of privacy, and**
 - the legal and political issues surrounding them.
- Privacy relates to: the *personal space* of user.
- Attention to privacy should include attention to: *public opinion*, user expectation, and thus user *perception and feelings*.

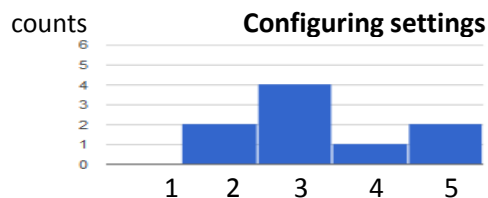
What do our users say / do?



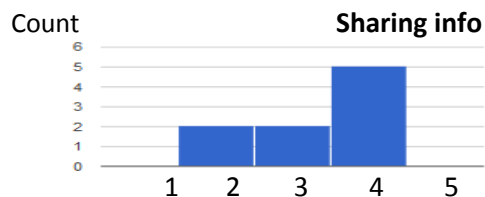
Privacy is on everyone's mind, and for quite a few it is a concern (4 on the scale of concern)



Understanding of technology behind privacy is typically high, and includes misconceptions



People don't configure privacy settings as much as they would like (caused by the hassle)



People are careful about what they share, but generally are ok sharing professional info in professional contexts with sites they trust

"I am more concerned with privacy in private life than in academic life, because the latter should be public"

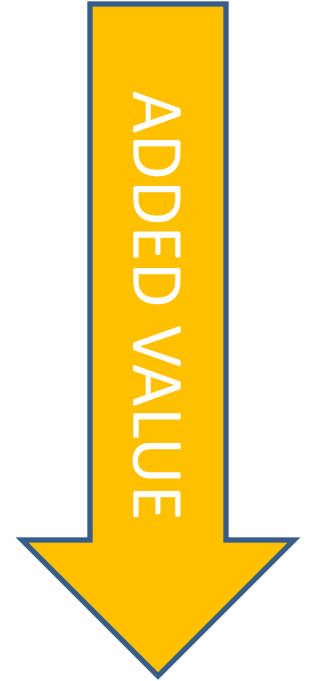
Variety of use of Personal Data

- Basic operation: providing access
- Improvements: analytics, A/B testing
- Management: account attribution
- Basic features: search history
- Personalization: e-mail alerts
- Added-value features: recommenders

(Research purposes)

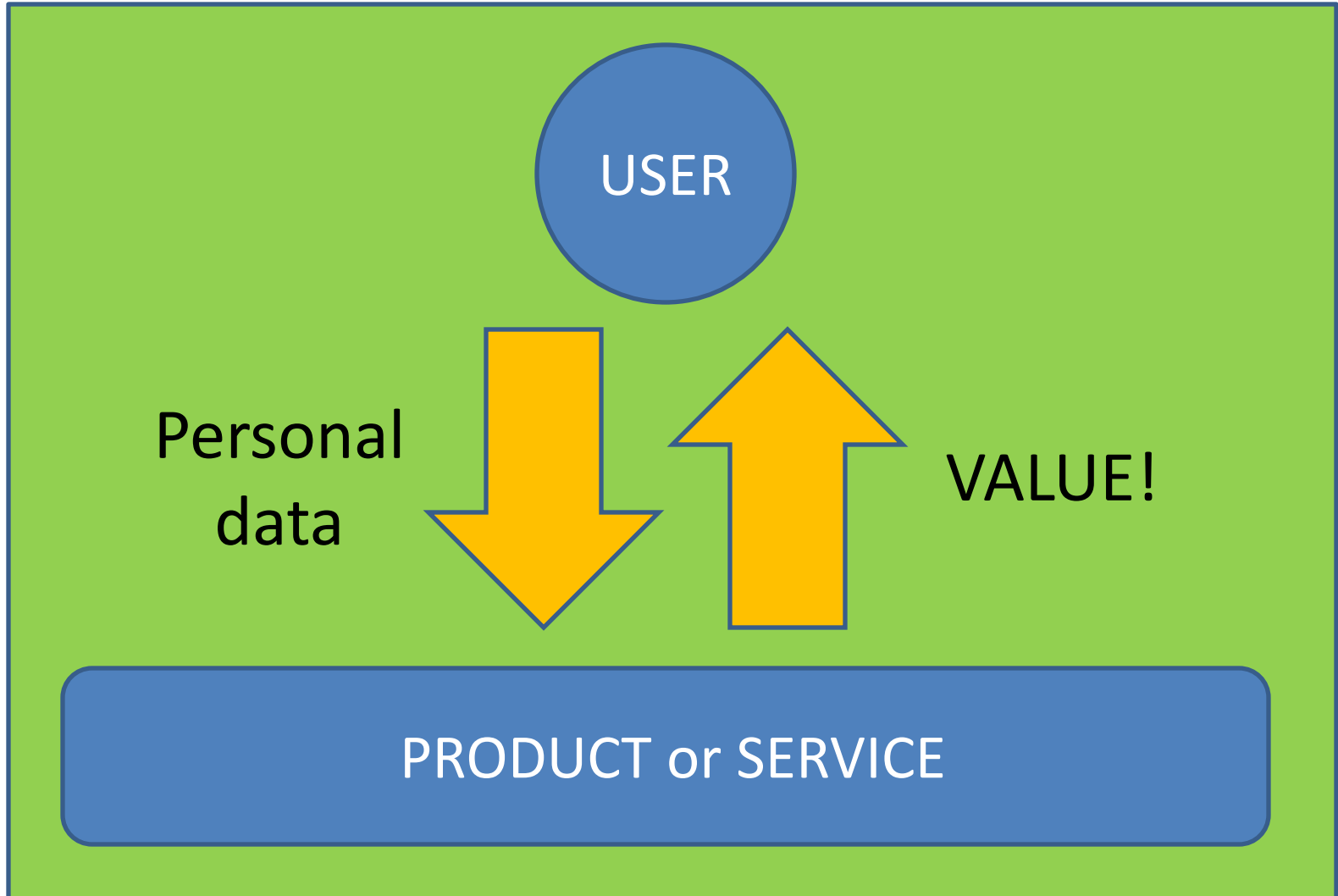
Variety of use of Personal Data

- Basic operation: providing access
- Improvements: analytics, A/B testing
- Management: account attribution
- Basic features: search history
- Personalization: e-mail alerts
- Added-value features: recommenders



(Research purposes)

User at center of Privacy



Responsibilities of product team

- Build trust from user through:
 1. Transparency
 2. Choice
 3. Added-value
- Corresponds with EU and NISO

Transparency

(Google Example)

your name, email address, telephone number or credit card to store with your account. If you want to take full advantage of the sharing features we offer, we might also ask you to create a publicly visible [Google Profile](#), which may include your name and photo.

- **Information we get from your use of our services.** We collect information about the services that you use and how you use them, like when you watch videos on YouTube, visit a website that uses our advertising, or interact with our ads and content. This information includes:

- **Device information**

We collect device-specific information (such as your operating system version, unique device identifiers or phone number) with your Google account.

- **Log information**

When you use our services or view content provided by Google, we automatically collect and store certain information in [server logs](#). This includes:

- details of how you used our service, such as your search queries.
- telephone log information like your phone number, calling-party

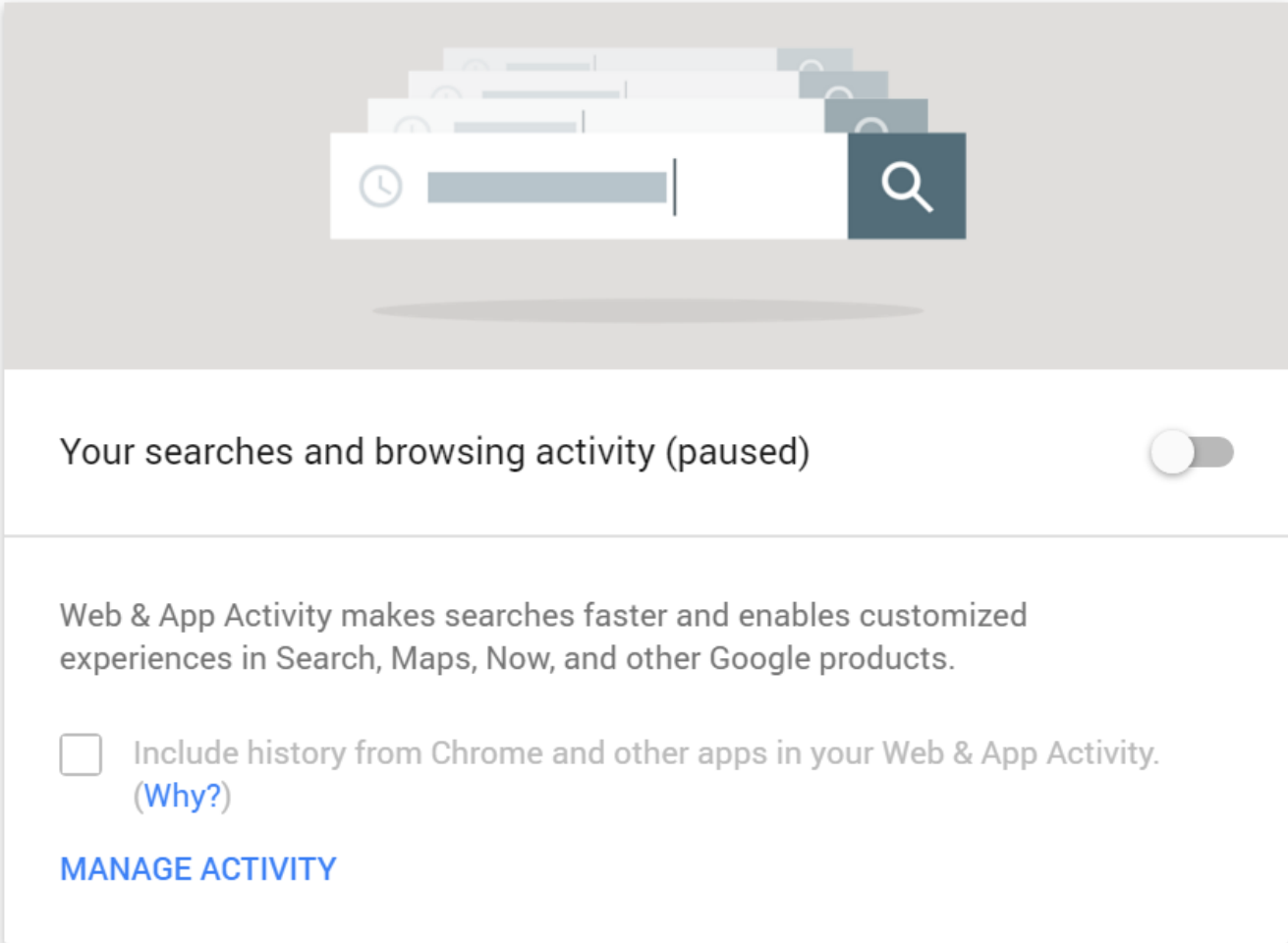
Example

For example, when you visit Google Play from your desktop, Google can use this information to help you decide on which devices you'd like your purchases to be available for use.


[Learn more.](#)

Choice and Added Value

(Google Example)



The image shows a screenshot of a Google settings page. At the top, there is a header with a search bar icon and a magnifying glass. Below this, the text reads "Your searches and browsing activity (paused)" followed by a toggle switch that is currently turned off. Underneath, there is a paragraph explaining that "Web & App Activity makes searches faster and enables customized experiences in Search, Maps, Now, and other Google products." Below this paragraph is a checkbox that is currently unchecked, with the text "Include history from Chrome and other apps in your Web & App Activity." and a link "(Why?)". At the bottom of the section, there is a blue link that says "MANAGE ACTIVITY".

Your searches and browsing activity (paused) 

Web & App Activity makes searches faster and enables customized experiences in Search, Maps, Now, and other Google products.

Include history from Chrome and other apps in your Web & App Activity. [\(Why?\)](#)

[MANAGE ACTIVITY](#)

Helper Guides

1. Privacy-by-design, with concepts like:
 - Respect for user privacy – keep it user-centric
 - Visibility and transparency – keep it open
 - Privacy embedded into design
 - End-to-end security – full lifecycle protection
2. Data Minimization: limit data collection and storage to what is necessary in relation to the purposes for which they are processed
3. Data aggregation and anonymization

User Privacy

- Needs attention, is not limiting
- Requires focus User and Trust
- Through transparency, choice, added-value

THANK YOU

questions?