

05. Protection from Web Tracking

Nataliia Bielova

[@nataliabelova](https://twitter.com/nataliabelova)

September 17th-21st, 2018

Web Privacy course

University of Trento

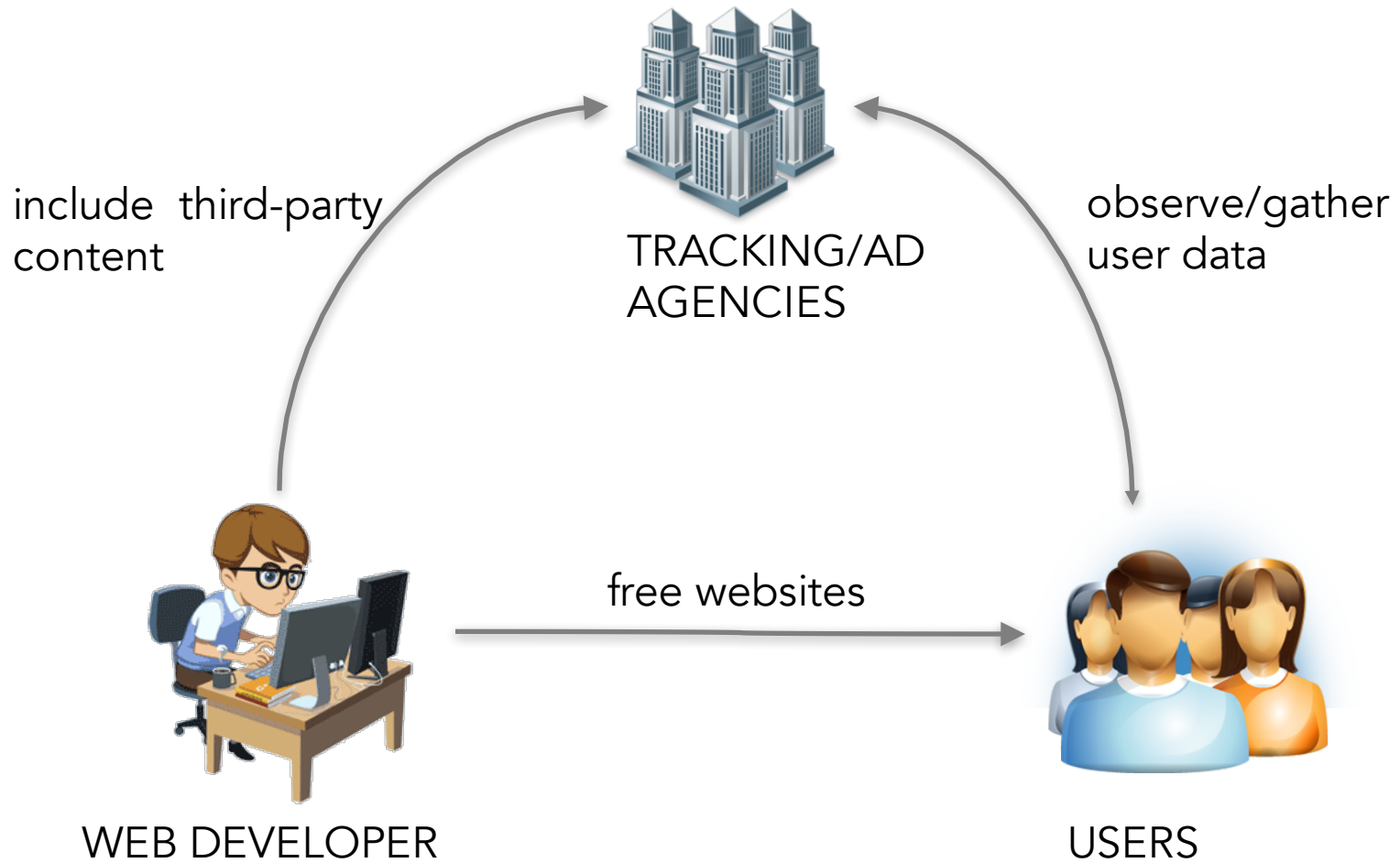
Today's class

- How to configure your browser to protect yourself from Web tracking?
- Private mode and Safari intelligent tracking protection
- Protection via browser extensions: ad blockers and tracking blockers
- Protection from browser fingerprinting



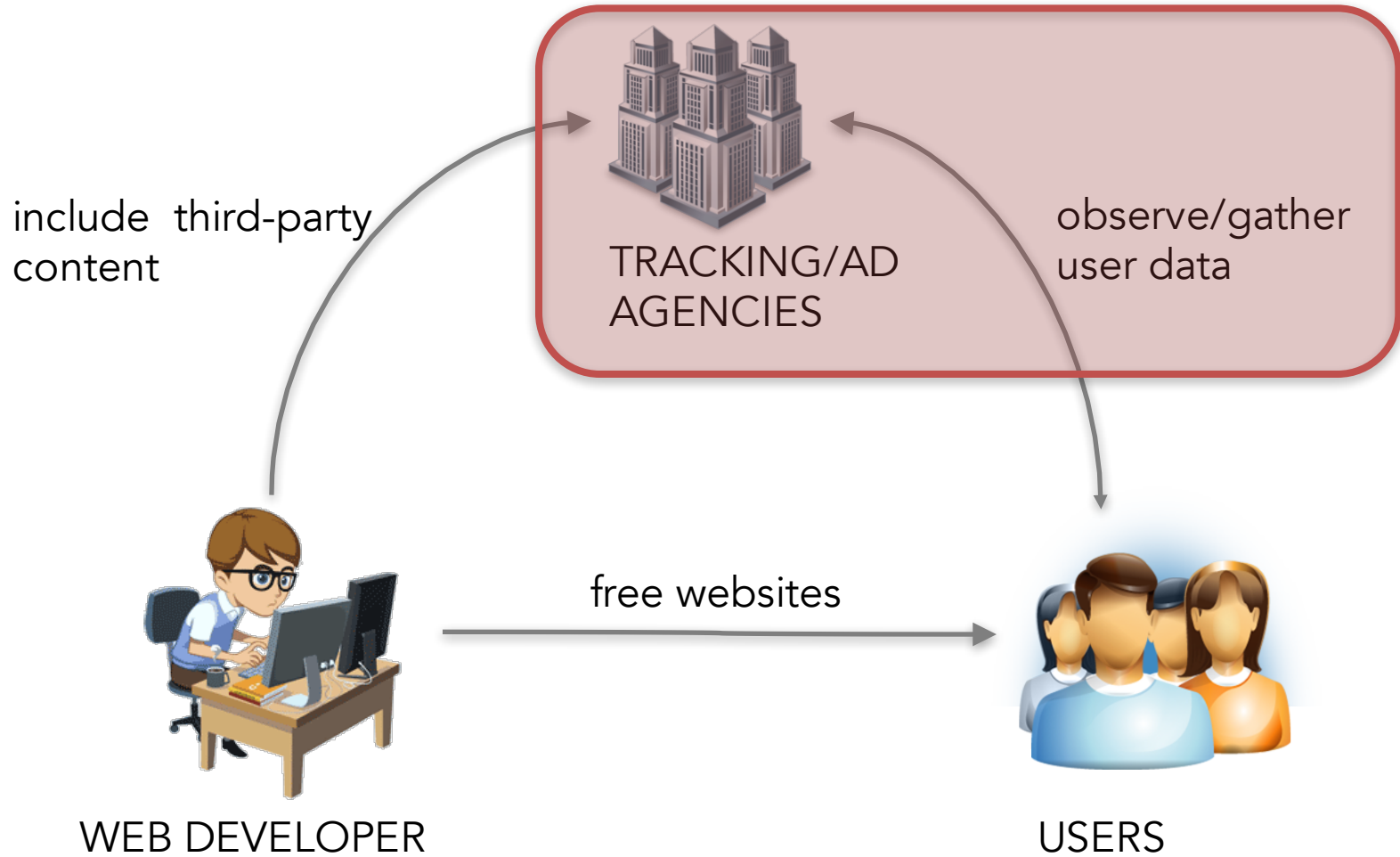
User protection from Web Tracking: Web browser configuration

Business model of the Web



Research Challenges

Detection and Measurement



Research Challenges

Detection and Measurement



TRACKING/AD
AGENCIES

observe/gather
user data

include third-party
content

Raising Awareness & Configuration

free websites

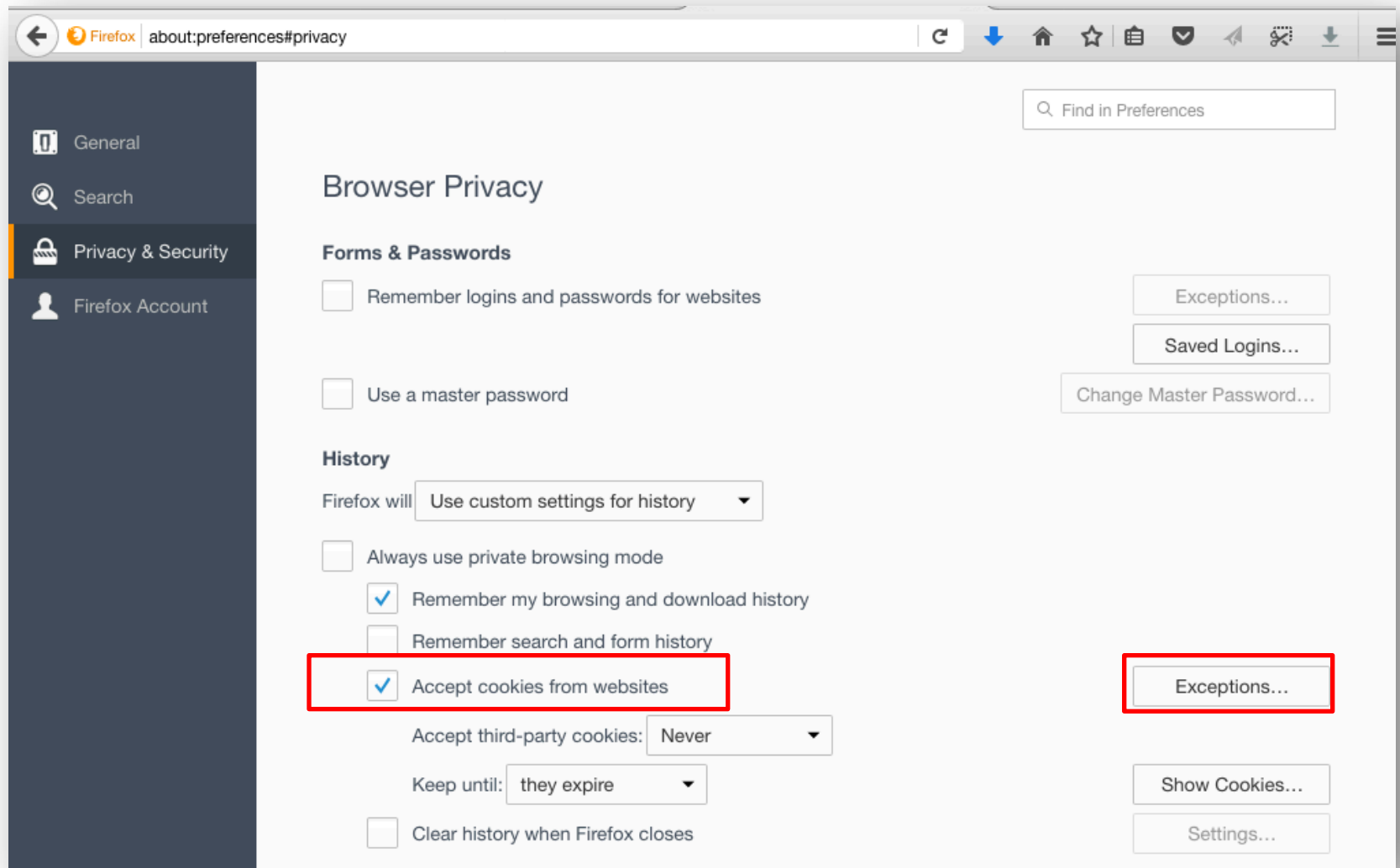


USERS



WEB DEVELOPER

First-party cookie setting



The screenshot shows the Firefox 'about:preferences#privacy' page. The left sidebar has 'Privacy & Security' selected. The main content area is titled 'Browser Privacy' and is divided into sections: 'Forms & Passwords', 'History', and 'Cookies'. In the 'Cookies' section, the checkbox 'Accept cookies from websites' is checked and highlighted with a red box. Below it, 'Accept third-party cookies' is set to 'Never' and 'Keep until' is set to 'they expire'. To the right of the 'Accept cookies from websites' checkbox is an 'Exceptions...' button, also highlighted with a red box. Other buttons like 'Exceptions...', 'Saved Logins...', 'Change Master Password...', 'Show Cookies...', and 'Settings...' are visible in the 'Forms & Passwords' and 'History' sections.

Firefox | about:preferences#privacy

Find in Preferences

Browser Privacy

Forms & Passwords

- Remember logins and passwords for websites [Exceptions...](#)
- Use a master password [Saved Logins...](#)
- [Change Master Password...](#)

History

Firefox will

- Always use private browsing mode
- Remember my browsing and download history
- Remember search and form history
- Accept cookies from websites [Exceptions...](#)

Accept third-party cookies:

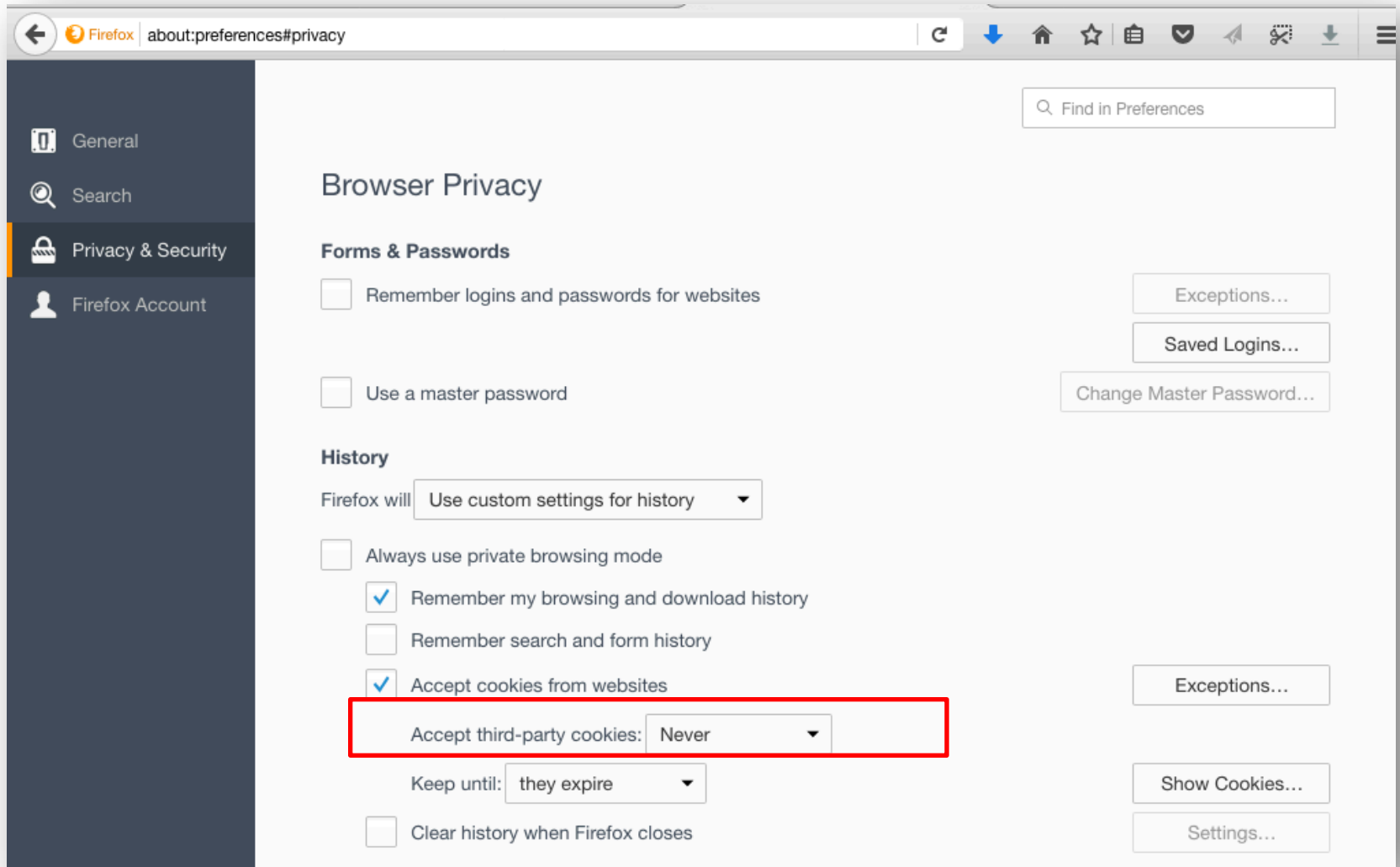
Keep until:

- Clear history when Firefox closes [Show Cookies...](#)
- [Settings...](#)

Do browser settings protect from within-site tracking?

- Browser setting: **block first-party cookies**
 - blocks setting cookies upon HTTP responses
 - blocks setting cookies via JavaScript
 - blocks reading cookies via JavaScript
 - **doesn't block** sending cookies via HTTP request if cookies are already in the browser (in Internet Explorer)

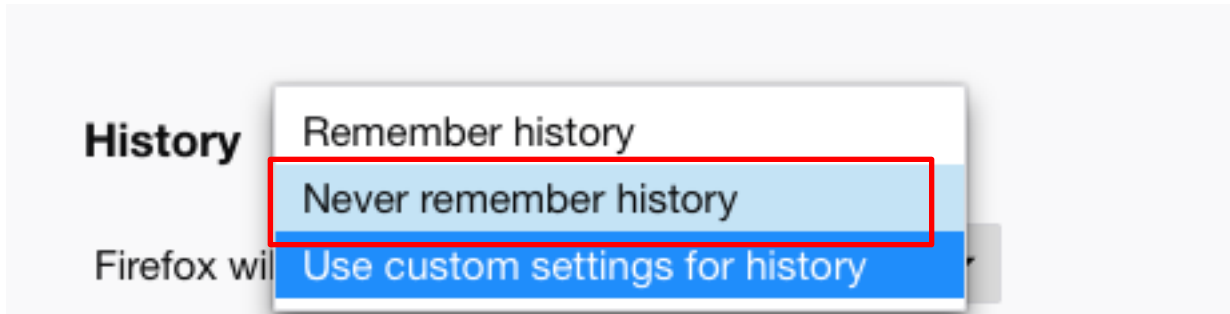
Third-party cookies blocking



Protection from stateful tracking

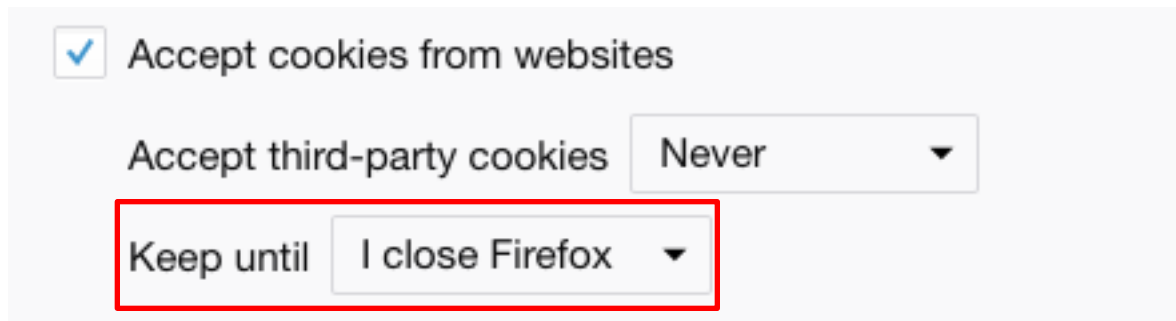
- Browser setting: **block third-party cookies**
 - Protects from tracking (purely) via cookies
 - Does not protect from cookie respawning
 - Does not protect from tracking via HTTP headers
 - In some browsers, as Internet Explorer

History browser settings



- Pros: protects from history stealing attacks
- Cons: doesn't protect from tracking

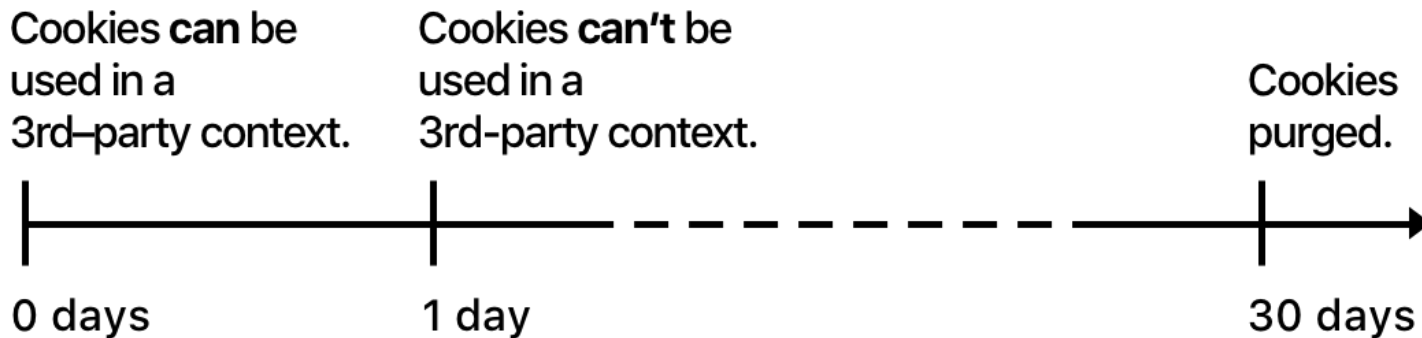
Delete cookies upon exiting



- Pros: protects from basic cookie tracking
- Cons: cookies can be restored via other storages, when logging in, via fingerprinting

Safari's Intelligent Tracking Protection

- affects whether a company can access first-party cookies in a **third-party context**



Days after the most recent interaction with the website.

Apple

No tracking, no revenue: Apple's privacy feature costs ad companies millions

Ad-tech firm Criteo likely to cut its 2018 revenue by more than a fifth after Apple blocked 'pervasive' tracking on web browser Safari

Alex Hern

🐦 @alexhern

Tue 9 Jan 2018 11.56 GMT



🕒 This article is over 3 months old

🔗
3510



▲ Apple said it is trying to combat information collected 'without permission and used for ad re-targeting'.
Photograph: Aly Song/Reuters

What about Private browsing mode?



You've gone incognito

Pages you view in incognito tabs won't stick around in your browser's history, cookie store, or search history after you've closed all of your incognito tabs. Any files you download or bookmarks you create will be kept.

However, you aren't invisible. Going incognito doesn't hide your browsing from your employer, your internet service provider, or the websites you visit.

[LEARN MORE](#)



Private Browsing with Tracking Protection

When you browse in a Private Window, Firefox **does not save**:

- visited pages
- cookies
- searches
- temporary files

Firefox **will save** your:

- bookmarks
- downloads

Private Browsing **doesn't make you anonymous** on the Internet. Your employer or Internet service provider can still know what page you visit.



Tracking Protection

Some websites use trackers that can monitor your activity across the Internet. With Tracking Protection Firefox will block many trackers that can collect information about your browsing behavior.

[See how it works](#)

How Private mode works?

- browsing history
- cookies
- searches
- ...



are stored only in the current separate “session”

Private mode is not so private...

- **Doesn't protect** from Web tracking across websites
- **Doesn't block** third-party cookies
 - neither in Firefox with Tracking protection ON
 - nor in Chrome
- **Browsing history can be merged** with other sessions
 - if the user logs in
 - via browser fingerprinting

Protection from Web tracking via browser extensions

(SEE SLIDES “EXTENSIONS”)

Protection from browser fingerprinting

(SEE SLIDES “FINGERPRINTING”)



GDPR and ePrivacy Regulations Tools for Web developers

Research Challenges

Detection and Measurement



TRACKING/AD
AGENCIES

observe/gather
user data

include third-party
content

Raising Awareness & Configuration

free websites



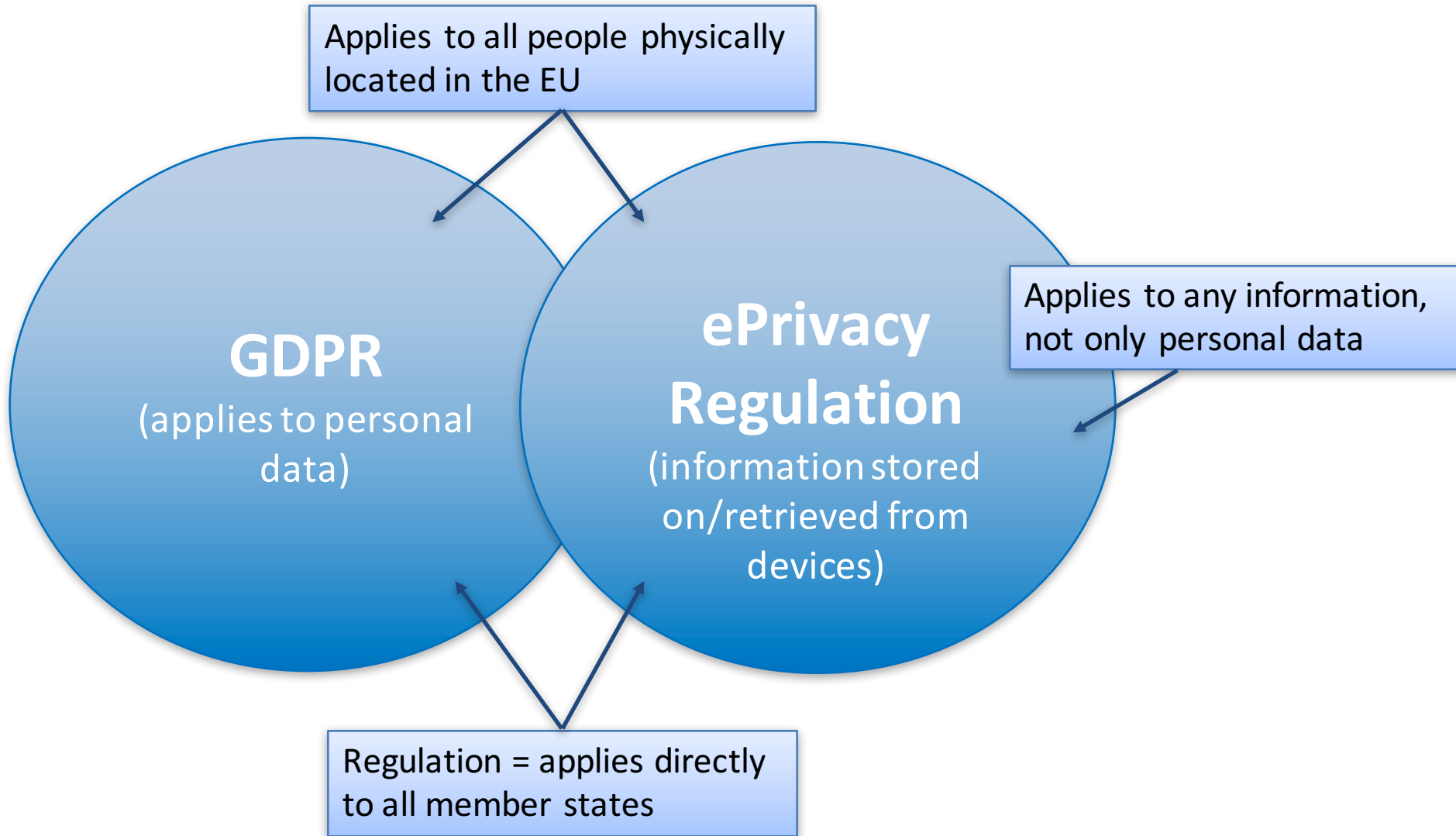
USERS



WEB DEVELOPER



EU Data Protection Regulations



Business model of the Web



include third-party
content



TRACKING/AD

observe/gather
user data

GDPR in force since May 25, 2018
ePrivacy Regulation under discussion



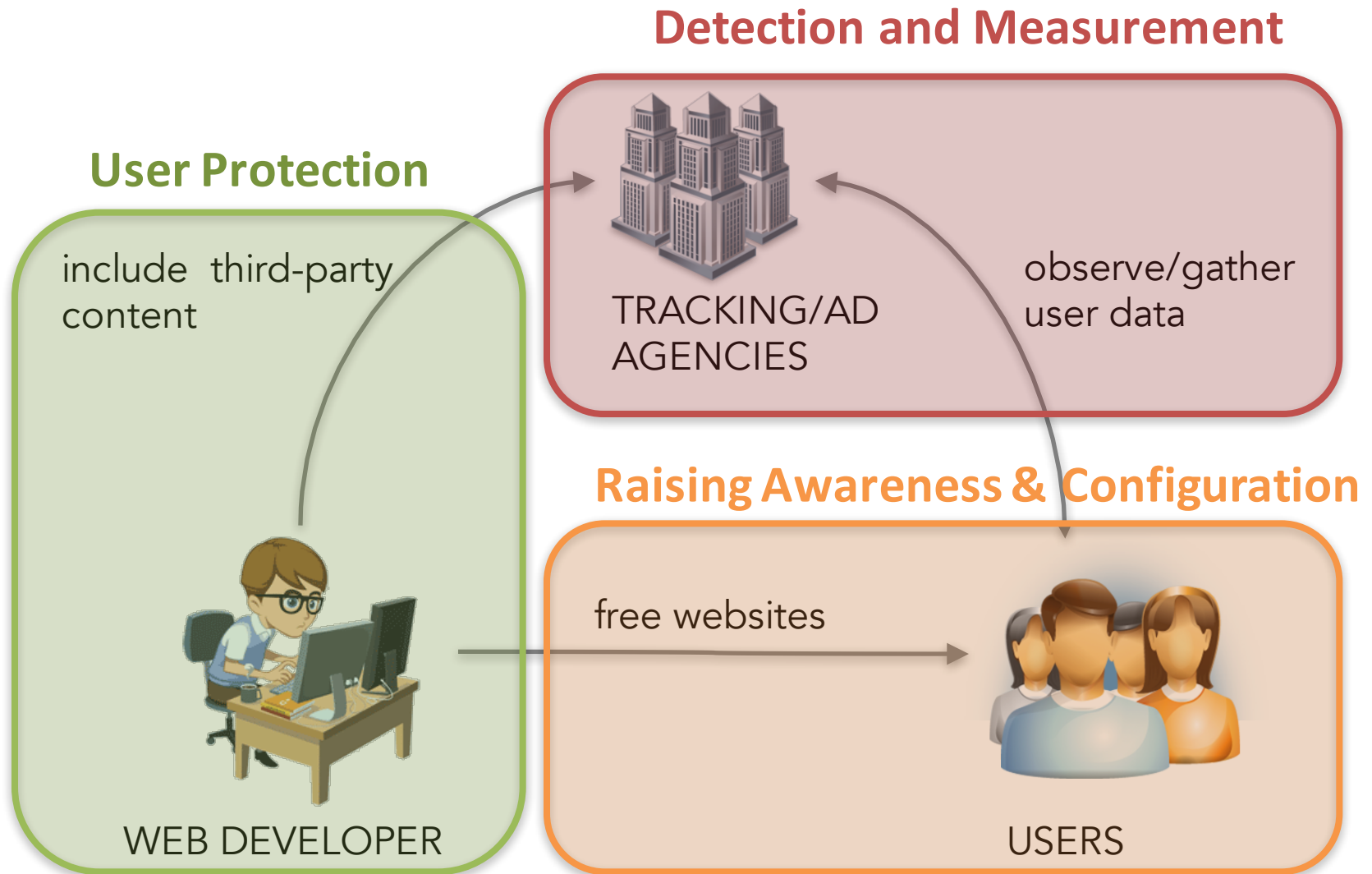
WEB DEVELOPER

free websites



USERS

Research Challenges



Why should web developers care about user protection?



- Current law:
 - **ePrivacy** directive 2009 (known as “cookie law”)

Why should web developers care about user protection?

thanks to ePrivacy directive 2009

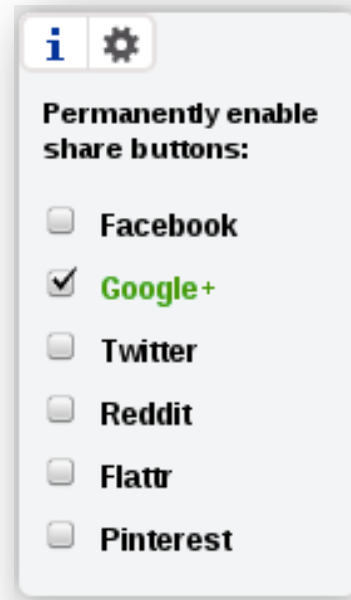
The screenshot shows a web browser displaying the AccuWeather website for Lyon, France. A green arrow points to a yellow cookie consent banner at the top of the page. The banner contains the text: "This site uses cookies. By continuing to browse the site you are agreeing to our use of cookies. Find out more here". Below the banner, the website header includes the AccuWeather logo, a search bar with "Lyon, France", and social media links. The main navigation bar shows "France Weather" and "Lyon, France 18°C". Below this, there are tabs for "Now 3:20 pm CEST", "Weekend", "Extended", "Month", "Radar", "MinuteCast®", and "Watch News". A banner for "eocofy" and "Newchic" shoes is displayed. The weather forecast section shows "CURRENT WEATHER" with a sun icon and "18°C RealFeel® 18° Sunny". It also shows "TODAY APR 16" with a sun and cloud icon, "19° Hi RealFeel® 18° A thunderstorm in spots", "TONIGHT APR 16" with a moon and cloud icon, "9° Lo RealFeel® 9° Turning out clear", and "TOMORROW APR 17" with a sun and cloud icon, "22° Hi RealFeel® 23° Partly sunny and pleasant". An advertisement for "catawiki" watches is also visible.

Why should web developers care about user protection?

- EU privacy regulations updated
 - **GDPR** (General Data Protection Regulation) 05/2018
 - **ePrivacy** Regulation ??/2020
- Companies **will have to implement a proper user consent** for information stored or accessed on user's browser
- **Fines**: up to **20M euro or 4% global annual turnover** (whatever is bigger) **per violation**

Want to include social buttons but not to track users?

Social Share Privacy



<http://panzi.github.io/SocialSharePrivacy/>

Third party content on websites

Today

- up **to 34 distinct third parties** on a single website [Lerner-etal-USENIX'16]
- 90% of content **is tracking users** [Roesner-etal-NSDI'12]
- Common protection: **client-side browser extensions**
 - Ghostery, Disconnect, AdBlockPlus, etc.

Tomorrow

- **ePrivacy Regulation**: website **owners are responsible** if third parties track their users
- Website owners want to control third-party content they include

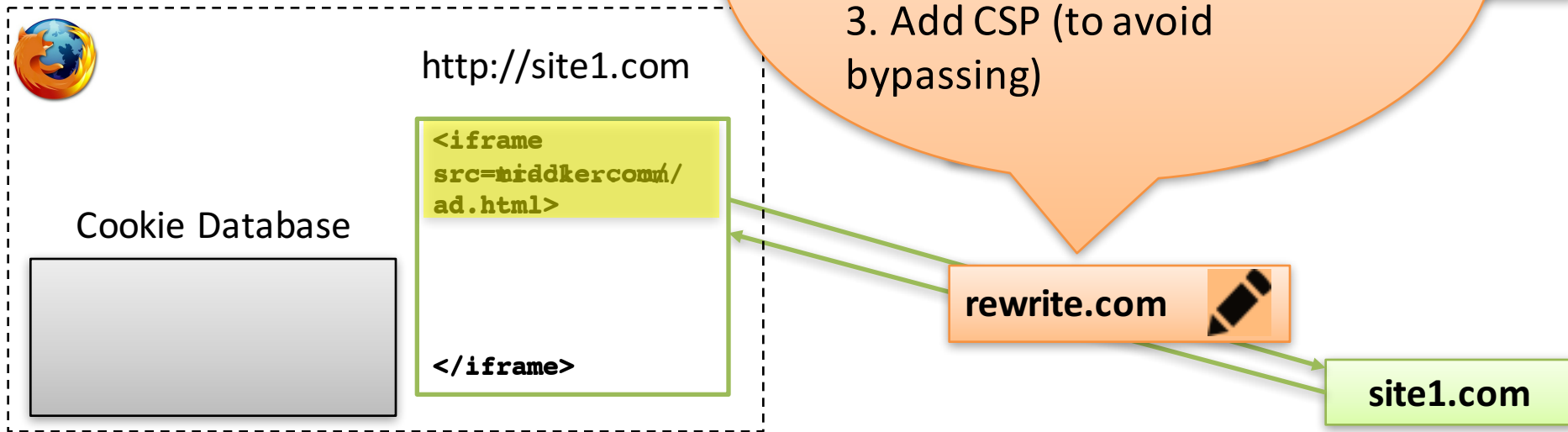
How to provide **automatic tools** for web applications developers to **include** third party content **without** third party tracking?



Control What You Include!

- First prototype that helps you control what you include
third-party content with

1. Redirect third parties to middle.com
2. Intercept dynamically created content
3. Add CSP (to avoid bypassing)

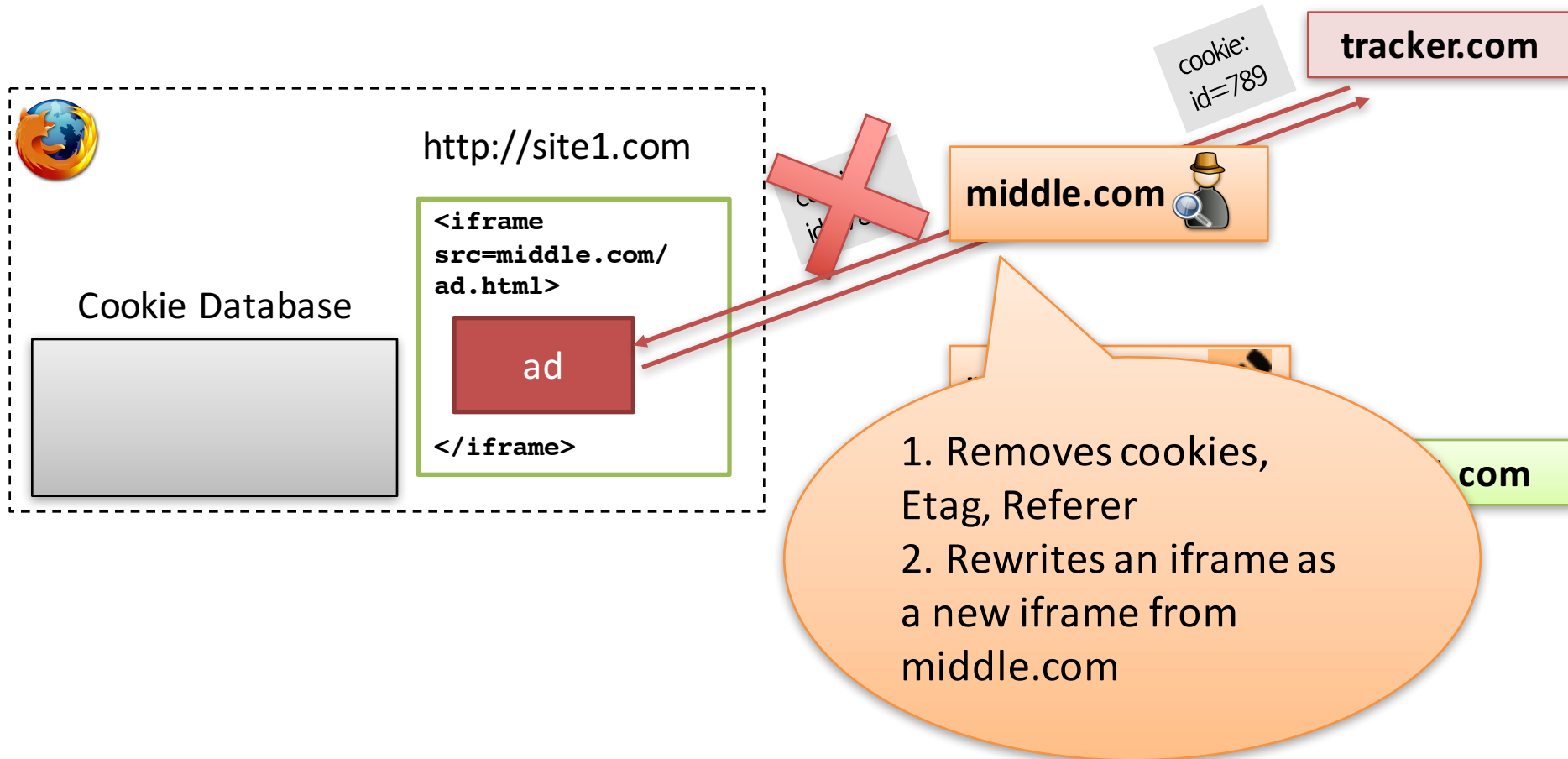


<http://tracker.com/smiley.gif> →
<http://middle.com/?url=http://tracker.com/smiley.gif>



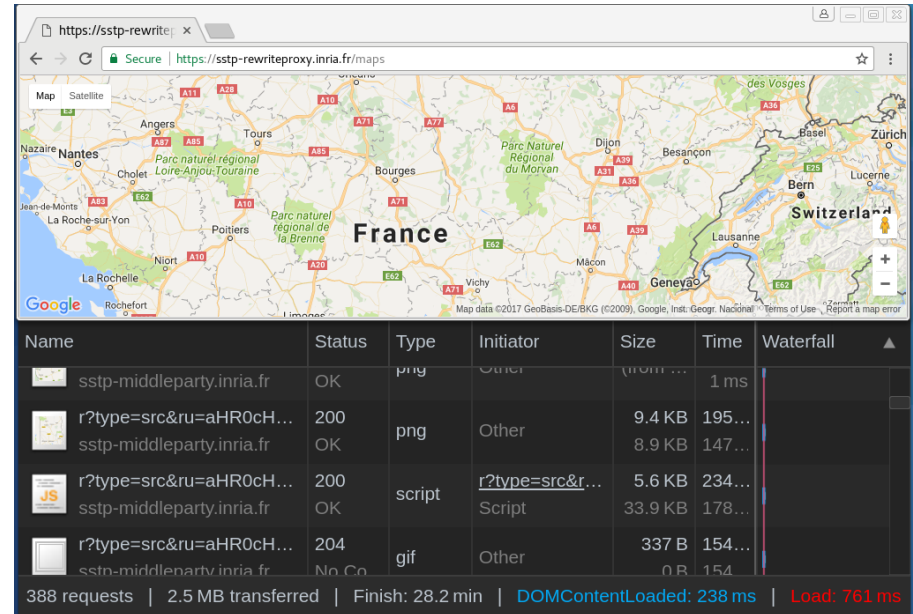
Control What You Include!

- First prototype that helps Web developers to **include third-party content without Web tracking**



Case Study

- Demo website:
 - Youtube videos
 - Google Map
 - Images, stylesheets
 - Videos, audios...



The screenshot shows a web browser window displaying a Google Map of France. Overlaid on the bottom half of the browser is a network monitoring tool interface. The interface includes a table with the following columns: Name, Status, Type, Initiator, Size, Time, and Waterfall. The table lists several requests to sstp-middleparty.inria.fr, including a 1 ms request, a 9.4 KB PNG image, a 5.6 KB script, and a 337 B GIF image. At the bottom of the interface, summary statistics are displayed: 388 requests, 2.5 MB transferred, Finish: 28.2 min, DOMContentLoaded: 238 ms, and Load: 761 ms.

Name	Status	Type	Initiator	Size	Time	Waterfall
ssstp-middleparty.inria.fr	OK	png	Script	9.4 KB	1 ms	
r?type=src&ru=aHR0cH...	200	png	Other	9.4 KB	195...	
ssstp-middleparty.inria.fr	OK	png	Other	8.9 KB	147...	
r?type=src&ru=aHR0cH...	200	script	r?type=src&r...	5.6 KB	234...	
ssstp-middleparty.inria.fr	OK	script	Script	33.9 KB	178...	
r?type=src&ru=aHR0cH...	204	gif	Other	337 B	154...	
ssstp-middleparty.inria.fr	No Co			0 B	154...	

388 requests | 2.5 MB transferred | Finish: 28.2 min | DOMContentLoaded: 238 ms | Load: 761 ms

The Middle Party Server successfully removes tracking