



# PRIVACY BY DESIGN

---

*Start by thinking privacy first*







# MICHELANGELO VAN DAM

---

- Web Application Architect
- CEO In2it
- President PHPBenelux
- Coach at CoderDojo
- Open source contributor
- Conference speaker

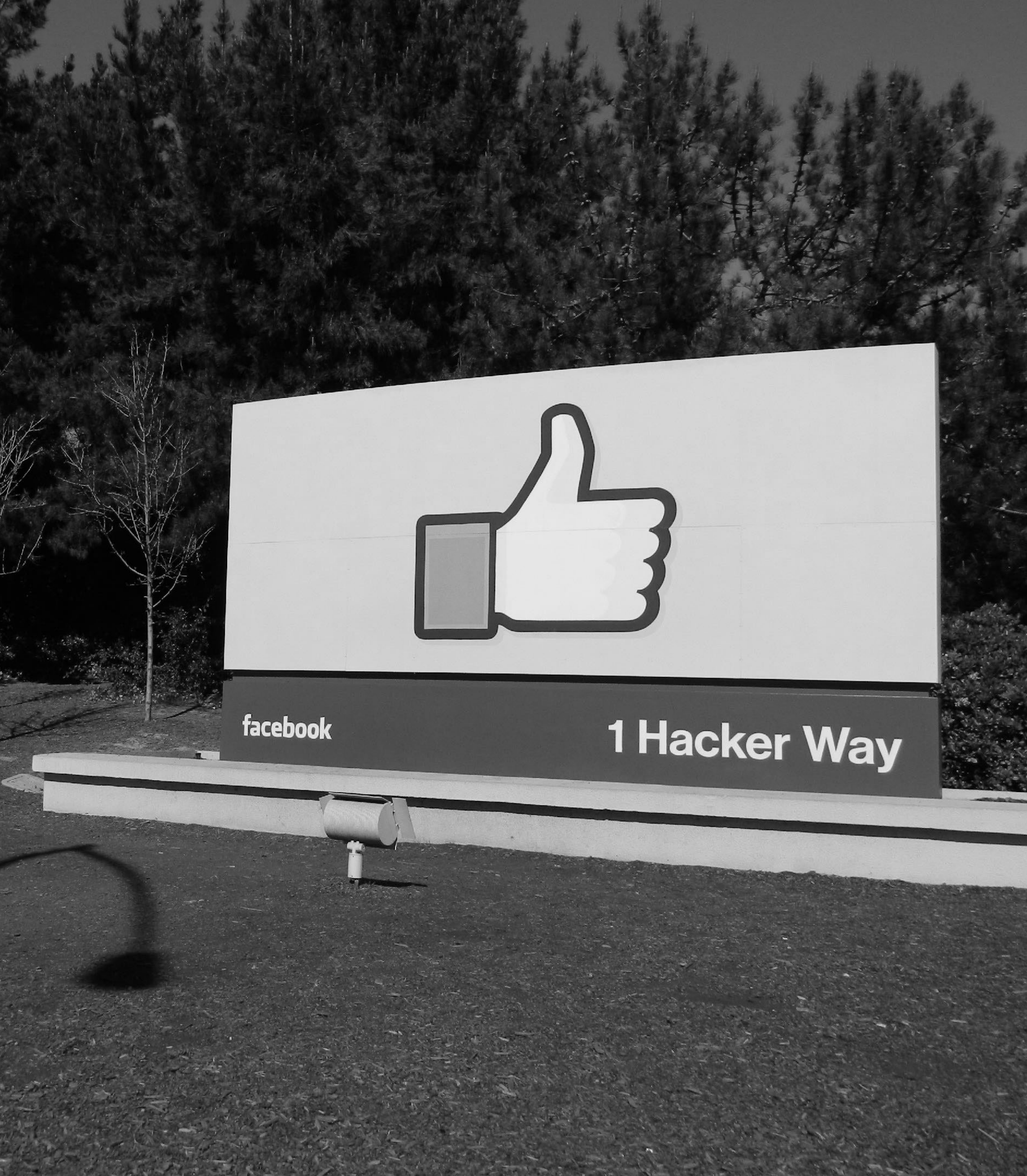




# WHY IS PRIVACY IMPORTANT?

---

- Human right
- Too much data already collected
- Information is everywhere
- Individuals have become the product





**Bupa employee steals 547,000 customers' data**

**Verizon partner data breach exposes millions of customer records**

*Accessed through an unprotected Amazon S3 storage server*

OCT 9, 2013 @ 12:57 PM 19,128

**After Security Breach Exposes 2.9 Million Adobe Users**

***Wells Fargo Accidentally Releases Trove of Data on Wealthy Clients***

Security sucks: measures often disabled to increase productivity



**Flight Centre leaks fliers' passport details to 'potential suppliers'**

Human error at travel company Flight Centre has resulted in a leak of personal information, including data of customers' passports. "Personal information relating to some leisure customers in Australia was accidentally made available to a small number of potential third party suppliers for a short period of time," a ...

Simon Sharwood, 13 days



# LATEST BREACHES THAT IMPACTED PEOPLE'S LIVES

---

**Equifax (2017)**

**143 Million accounts hacked**  
financial exposure (credit), credit card data & personal information

**Ashley Madison (2015)**

**37 Million accounts hacked**  
extortion, divorces, suicides

**OPM (2015)**

**21 Million US government personnel**  
foreign assets, informant data, addictions & relationship issues







Password:

# YOUR ADVERSARIES

---

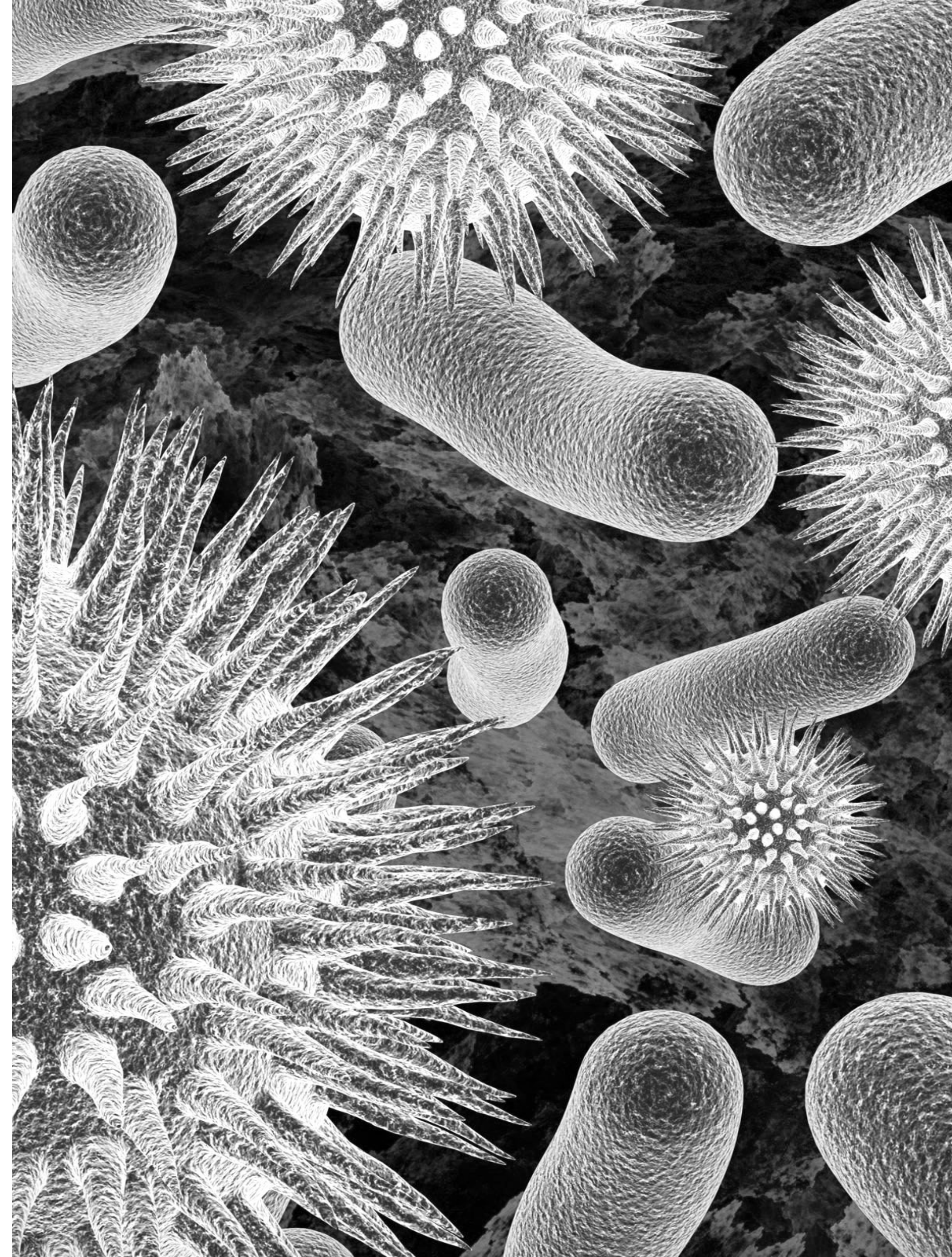
*Who's after your data?*



# VIRUSES

---

*Automated scripts to steal data*





# SCRIPT KIDDIES

---

*Using free tools and often have no clue  
what they're doing*





# SOFTWARE ENGINEERS

---

*These people are new to security and try  
out things they have learned*





# PROFESSIONALS

---

*They are the security experts!*





# COMPETITION

---

*They're after your secret sauce*





# NATION STATES

---

*They might already be inside ...*





# EMPLOYEES

---

*They have all the access!*





# WHAT IF

---

*A service I use has been breached?*



[Home](#)[Notify me](#)[Domain search](#)[Who's been pwned](#)[Passwords](#)[API](#)[About](#)[Donate !\[\]\(17413706fd4997a1a4bdf85c6864eee1\_img.jpg\) !\[\]\(f419710cbe076aa30a9c6c031b5cbe84\_img.jpg\)](#)

# ';--have i been pwned?

Check if you have an account that has been compromised in a data breach

pwned?

252

pwned websites

4,820,896,763

pwned accounts

57,485

pastes

55,449,811

paste accounts

## Top 10 breaches



711,477,622 Onliner Spambot accounts




593,427,119 Exploit.In accounts ?



457,962,538 Anti Public Combo List accounts ?




393,430,309 River City Media Spam List accounts 



# Oh no — pwned!

Pwned on 5 [breached sites](#) and found no [pastes](#) ([subscribe](#) to search sensitive breaches)

 [Notify me when I get pwned](#)

 [Donate](#)



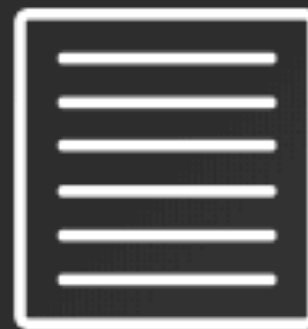
## Breaches you were pwned in

A "breach" is an incident where a site's data has been illegally accessed by hackers and then released publicly. Review the types of data that were compromised (email addresses, passwords, credit cards etc.) and take appropriate action, such as changing passwords.



**Adobe:** In October 2013, 153 million Adobe accounts were breached with each containing an internal ID, username, email, *encrypted* password and a password hint in plain text. The password cryptography was poorly done and many were quickly resolved back to plain text. The unencrypted hints also disclosed much about the passwords adding further to the risk that hundreds of millions of Adobe customers already faced.

**Compromised data:** Email addresses, Password hints, Passwords, Usernames



**Exploit.In (unverified):** In late 2016, a huge list of email address and password pairs appeared in a "combo list" referred to as "Exploit.In". The list contained 593 million unique email addresses, many with multiple different passwords hacked from various online systems. The list was broadly circulated and used for "credential stuffing", that is attackers employ it in an attempt to identify other online systems where the account owner had reused their password. For detailed background on this incident, read [Password reuse, credential stuffing and another billion records in Have I been pwned](#).

**Compromised data:** Email addresses, Passwords



**Last.fm:** In March 2012, the music website [Last.fm](#) was hacked and 43 million user accounts were exposed. Whilst [Last.fm](#) knew of an incident back in 2012, the scale of the hack was not known until the data was released publicly in September 2016. The breach included 37 million unique email addresses, usernames and passwords stored as unsalted MD5 hashes.

**Compromised data:** Email addresses, Passwords, Usernames, Website activity





# HOW TO PROTECT PRIVACY?

---

*Time to step up and give trust back to your customers*





# DON'T COLLECT ALL THE THINGS!

---

*Keep it to a bare minimum*





# LIMIT EXPIRATION

---

*Don't keep longer than needed*





# SEPARATE

---

*Keep private information somewhere  
different from other (business) data*





# DON'T EXPOSE

---

*Keep private data hidden from views*





# SERVICE BINGO





MailChimp





# DO YOU HAVE AN AGREEMENT WITH YOUR SERVICE PROVIDER?

---

## CONFIDENTIAL

### Customer EU Data Processing Addendum

This Data Processing Addendum ("DPA"), forms part of the Agreement between The Rocket Science Group LLC d/b/a MailChimp ("MailChimp") and \_\_\_\_\_ ("Customer") and shall be effective on the date both parties execute this DPA ("Effective Date"). All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement.

#### 1. Definitions

"Affiliate" means an entity that directly or indirectly Controls, is Controlled by or is under common Control with an entity.

"Agreement" means MailChimp's Terms of Use, which govern the provision of the Services to Customer, as such terms may be updated by MailChimp from time to time.

"Control" means an ownership, voting or similar interest representing fifty percent (50%) or more of the total interests then outstanding of the entity in question. The term "Controlled" shall be construed accordingly.

"Customer Data" means any Personal Data that MailChimp processes on behalf of Customer as a Data Processor in the course of providing Services, as more particularly described in this DPA.



# SOME EXAMPLES

*Technical things you can do right now!*





# “SECRETS” MANAGEMENT


Repositories	535
Code	284K
Commits	320K
Issues	7K
Topics	
Wikis	1K
Users	

Languages	
PHP	X
Blade	265

[Advanced search](#) [Cheat sheet](#)


284,151 code results

Sort: Best match ▾

 theowni/encryptedSession-PHP – \_secret\_key.php PHP


Showing the top three matches Last indexed on 19 Sep 2016

```
1 <?php $secret_key = "5627702d35ce7016589009398cdf3e81c469871ee5c62da5d14f8277f712d0fb";
   $secret_key = pack("H*", $secret_key); ?>
```

 mejiagarcia/PHP-JWT-TOKEN-API – config.php PHP

Showing the top match Last indexed on 28 Apr 2017

```
1 <?php
2 $secret_key = "52e29fc7d1d38d35281e320c3cc1e5a4";
3 ?>
```

 eugenesisdash/sasdada.gr.dev – variable\_secret\_key.php PHP


Showing the top match Last indexed on 24 Oct 2017

```
1 <?php
2     $secret_key = '7172606872131q';
3 ?>
```

 bigrocs/shopmall – key.php PHP

Showing the top match Last indexed on 25 Sep 2016

```
1 <?php $secret_key = "c0019dfa2ab0effcfd4bb3824c6c8677";?>
```

 BlackFireOne/blackfireonee.github.io – variable\_secret\_key.php PHP

Showing the top match Last indexed on 24 Sep 2016

```
1 <?php
2     $secret_key = '7172606872131q';
3 ?>
```



# PROTECT YOUR SECRETS

---



CYBERARK®  
**conjur**



**amazon**  
web services™



HashiCorp  
**Vault**



# HASHICORP VAULT

---

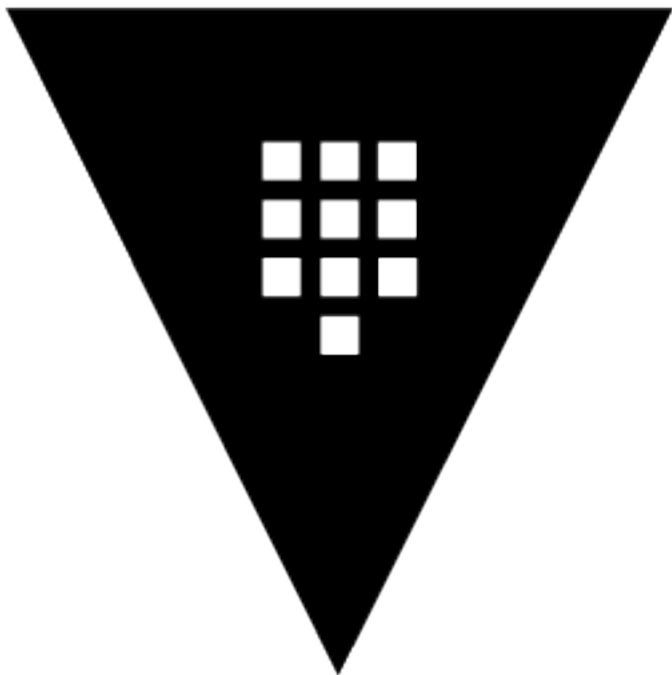
- Tool for managing secrets
  - [vaultproject.io](https://vaultproject.io)
- Secures, stores and controls
  - access tokens
  - passwords
  - certificates
  - API keys
  - ... others
- Access Control
  - Key Rolling
  - Configurable lease time
  - Audit logs
  - Open Source



Application  
Tokens

Database  
credentials

Audit  
logs



HashiCorp  
**Vault**

Stored  
Secrets

Cloud  
Temp keys

ACL's



# EXAMPLE: TEMPORARY AWS ACCOUNT

aws

Services

Resource Groups

Michelangelo van Dam

Global

Add user

Delete user

Find users by username or access key

	User name	Groups	Access key age	Password age	Last activity
<input type="checkbox"/>	vault-root-d...	None	Today	None	

```
~/vd vault read aws/creds/developer
Key      Value
---      -
lease_id aws/creds/developer/feeed9b3-ad0d-05db-aa32-f8da411e6d
6c
lease_duration 768h
lease_renewable true
access_key      AKIAJK3V4XONNWBTR7UA
secret_key      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
security_token  <nil>
~/vd
```

Feedback

English (US)

© 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Privacy Policy



## 2. DragonBe's Haunted Terminal (mysql)

```
---      -----
lease_id      database/creds/reader/bab70e22-c67b-b5df-a60b-2eb364cf97f5
lease_duration 1h0m0s
lease_renewable true
password       A1a-pp5uqzzu63qqy59p
username       v-root-reader-396urs6vpuywyx77

mysql -uv-root-reader-396urs6vpuywyx77 -p vault_demo
Enter password:
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 14
Server version: 5.7.19 MySQL Community Server (GPL)

Copyright (c) 2000, 2017, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> █
```



# USE A TEAM PASSWORD MANAGER

**1Password**

**LastPass...**

**RoboForm**

 **dashlane**



# GIVE 2FA TO EVERYONE!





# AUDIT TRAILS WITH MIDDLEWARE & CQRS

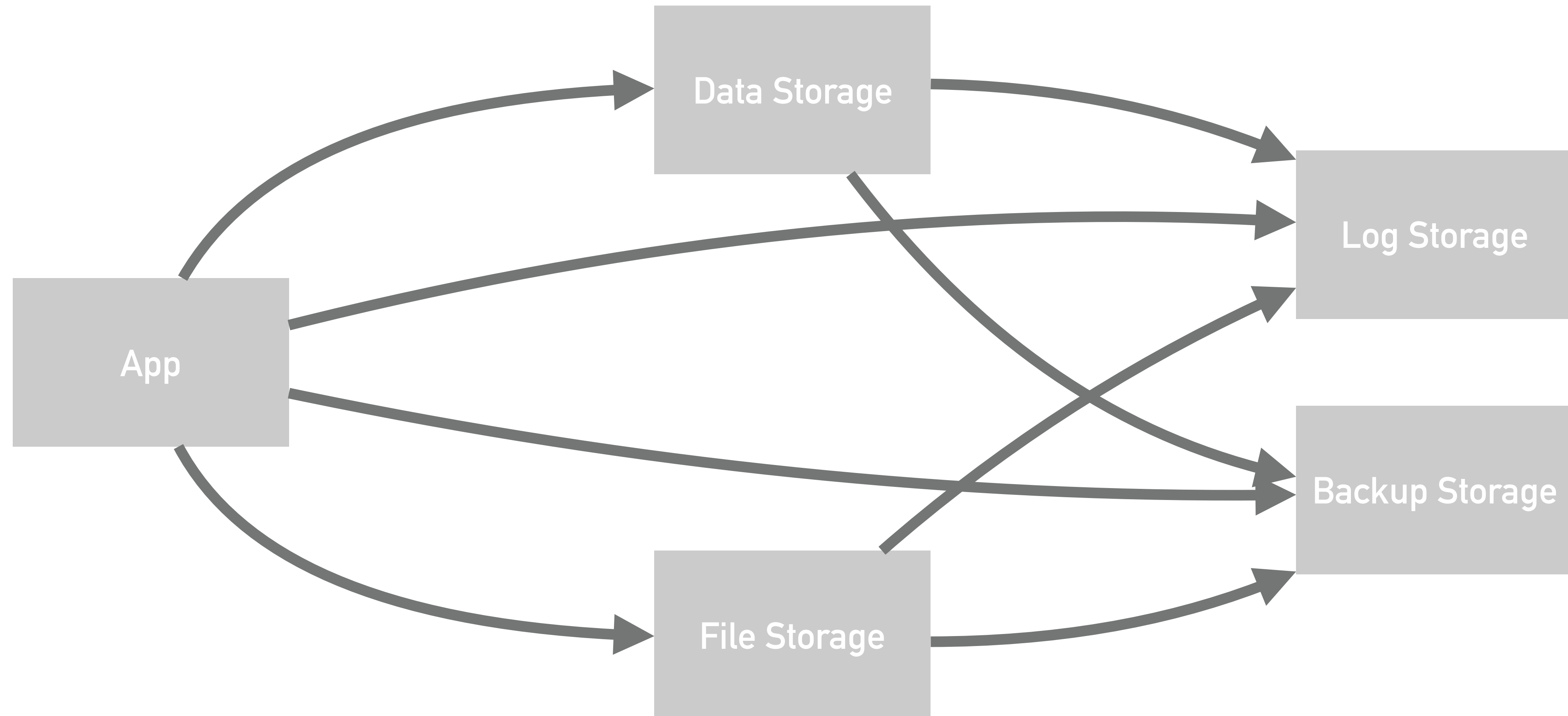
---

- Log access to data
- Automate anonymising of privacy data
- Automate encryption of privacy data



# ...AND DON'T FORGET TO ENCRYPT YOUR STORAGE & COMMUNICATIONS!

---



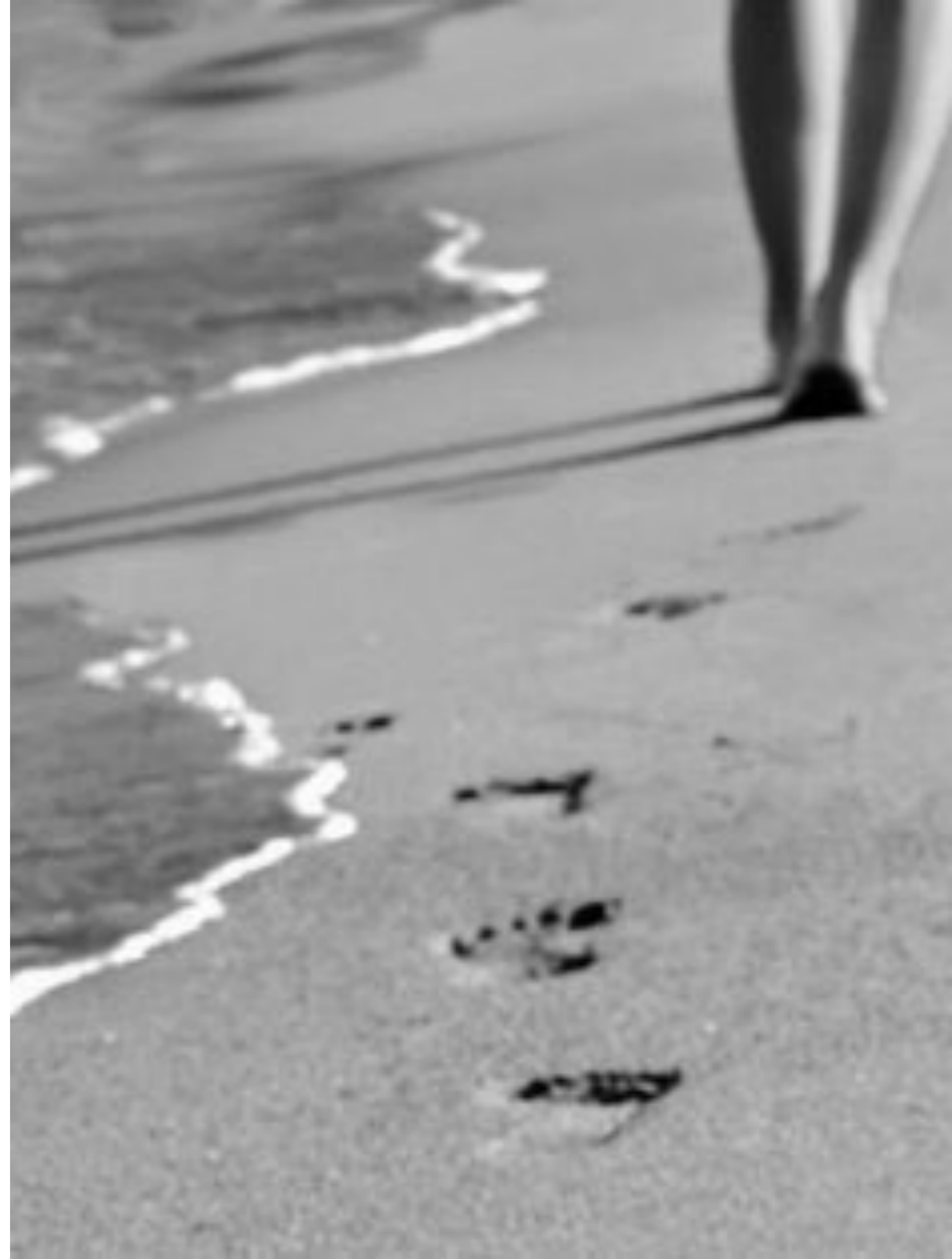
*Public - private key exchange | encrypted data storage*



# WHAT YOU CAN DO NOW!

---

*Simple steps towards more privacy*







# RESPECT DNT HEADERS

---

*Your users have chosen to opt-out*





Google Chrome may use web services to improve your browsing experience. You may optionally disable these services. [Learn more](#)

Use a web service to help resolve navigation errors



Use a prediction service to help complete searches and URLs typed in the address bar



Use a prediction service to load pages more quickly



Automatically send some system information and page content to Google to help detect dangerous apps and sites



Protect you and your device from dangerous sites



Automatically send usage statistics and crash reports to Google



Send a "Do Not Track" request with your browsing traffic



Use a web service to help resolve spelling errors



Smarter spell-checking by sending what you type in the browser to Google

Manage certificates

Manage HTTPS/SSL certificates and settings





**Accept:** text/html,application/xhtml+xml,application/xml;q=0.9

**Accept-Encoding:** gzip, deflate, br

**Accept-Language:** en-GB,en;q=0.8,en-US;q=0.6,nl;q=0.4

**Cache-Control:** max-age=0

**Connection:** keep-alive

**DNT:** 1

**Host:** www.example.com

**Upgrade-Insecure-Requests:** 1

**User-Agent:** Mozilla/5.0 (<script>alert('Filter Input, Escape Output');</script>)



## Apache Environment

Variable	Value
SCRIPT_URL	/~teraisan/K1053BI/examples/phpinfo.php
SCRIPT_URI	http://www.oamk.fi/~teraisan/K1053BI/examples/phpinfo.php
HTTP_HOST	www.oamk.fi
HTTP_CONNECTION	keep-alive
HTTP_UPGRADE_INSECURE_REQUESTS	1
HTTP_ACCEPT	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
HTTP_USER_AGENT	Mozilla/5.0 (iPhone; CPU iPhone OS 11_0_3 like Mac OS X) AppleWebKit/604.1.38 (KHTML, like Gecko) Version/11.0 Mobile/15A432 Safari/604.1
HTTP_ACCEPT_LANGUAGE	en-us
HTTP_DNT	1
HTTP_ACCEPT_ENCODING	gzip, deflate
PATH	/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
SERVER_SIGNATURE	<i>no value</i>
SERVER_SOFTWARE	Apache
SERVER_NAME	www.oamk.fi
SERVER_ADDR	193.167.100.88
SERVER_PORT	80
REMOTE_ADDR	81.82.233.118
DOCUMENT_ROOT	/opt/www/docs_new/
REQUEST_SCHEME	http
CONTEXT_PREFIX	<i>no value</i>
CONTEXT_DOCUMENT_ROOT	/opt/www/docs_new/
SERVER_ADMIN	webmaster@oamk.fi
SCRIPT_FILENAME	/home/kaha/teraisan/public_html/K1053BI/examples/phpinfo.php
REMOTE_PORT	46156
GATEWAY_INTERFACE	CGI/1.1
SERVER_PROTOCOL	HTTP/1.1
REQUEST_METHOD	GET
QUERY_STRING	<i>no value</i>
REQUEST_URI	/~teraisan/K1053BI/examples/phpinfo.php
SCRIPT_NAME	/~teraisan/K1053BI/examples/phpinfo.php



# INTERESTING FOR DISABLING GOOGLE ANALYTICS

---

```
<?php if (!array_key_exists('HTTP_DNT', $_SERVER) || 1 !== (int) $_SERVER['HTTP_DNT']): ?>
<!-- show your Google Analytics Script Here -->
<?php endif ?>
```






# COOKIE LAW

---

*The reason and nonsense applied*





**I Agree** ☐

## WHY CONSENT IS NECESSARY

---

- Your web server stores data on the client
- Cookie contains “unknown data”
- Cookie can be used to
  - Track user
  - Keep state of settings
  - Make references
- User is “unaware” of these methods
- Actions can be used to “profile” the user





*It's like someone drops something in your bag for which you get arrested and put in jail for...*



```
~ curl -c cookie.jar -b cookie.jar -I https://www.studio100.com
```

```
HTTP/2 302
```

```
date: Sat, 10 Mar 2018 15:01:29 GMT
```

```
content-type: text/html; charset=UTF-8
```

```
set-cookie: __cfduid=dd824f050df012b2aac793556ebf3b2ae1520694089; expires=Sun, 10-Mar-19 15:01:29 GMT; path=/; domain=.studio100.com; HttpOnly
```

```
cache-control: private, must-revalidate
```

```
pragma: no-cache
```

```
expires: -1
```

```
set-cookie: laravel_session=eyJpdiI6ImhWOFIwQWlpOHQyS0ZBckJqNnBaWnc9PSIsInZhbnHVlIjoiUmVsVkhwRXZxRHpwS0FPd1MxY1hmVnN5RjRMVWtjcW4ySk5qN3ZvUFwvVWFPbE0xZmloWHRLakhmazNVbmhkRzBxYU9BbGJxRDFkRXF0d0xVankrem1BPT0iLCJtYWMiOiI1YTVkZmM0ZDUwYzI0ZjIwYzUwZGZlMDg5MjVjMzUyNWRhNWRmYTg0ZTQ0ODRjMDA2ZmUwMzQ0MGQwODZkZmU5In0%3D; expires=Sat, 10-Mar-2018 17:01:29 GMT; Max-Age=7200; path=/; HttpOnly
```

```
location: https://studio100.com
```

```
age: 0
```

```
x-varnish-cache: uncached
```

```
expect-ct: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
```

```
server: cloudflare
```

```
cf-ray: 3f96a82a3eae443f-BRU
```

```
~ cat cookie.jar
```

```
# Netscape HTTP Cookie File
```

```
# https://curl.haxx.se/docs/http-cookies.html
```

```
# This file was generated by libcurl! Edit at your own risk.
```

```
#HttpOnly_.studio100.com      TRUE      /          FALSE     1552230089      __cfduid      dd824f050df012b2aac793556ebf3b2ae1520694089
```

```
#HttpOnly_www.studio100.com   FALSE     /          FALSE     1520701289      laravel_session eyJpdiI6ImhWOFIwQWlpOHQyS0ZBckJqNnBaWnc9PSIsInZhbnHVlIjoiUmVsVkhwRXZxRHpwS0FPd1MxY1hmVnN5RjRMVWtjcW4ySk5qN3ZvUFwvVWFPbE0xZmloWHRLakhmazNVbmhkRzBxYU9BbGJxRDFkRXF0d0xVankrem1BPT0iLCJtYWMiOiI1YTVkZmM0ZDUwYzI0ZjIwYzUwZGZlMDg5MjVjMzUyNWRhNWRmYTg0ZTQ0ODRjMDA2ZmUwMzQ0MGQwODZkZmU5In0%3D
```







*Time for  
Change*





# Hello, world!

Thank you for trusting us

## Cookie consent



We're using cookies to offer you a rich user experience as we store your preferences during your stay with us (session) and to analyse your visit on our website so we can improve our services to offer you a more personalised experience.

- **FOOBAR\_CONSENT:** A cookie that will be set once you have given us your consent to exchange cookies with you.
- **FOOBAR:** Our session cookie that we will use only for the duration of your stay with us (your session) so we can provide you access to your personal account, you language settings and other preferences you have set on our website.

Accept

Close

Elements

Console

Application

Sources

Network

Performance

Memory

Security

Audits

Adblock Plus

Local Storage

Session Storage

IndexedDB

Web SQL

Cookies

http://localhost:8000

Cache

Cache Storage

Application Cache

Filter

Name	Value	Domain	Path	Expires / Max-Age	Size	HTTP	Secure	SameSite

Console

Network conditions

top

Filter

Default levels

Group similar



# Hello, world!

Thank you for trusting us

Elements

Console

Application

Sources

Network

Performance

Memory

Security

Audits

Adblock Plus

Local Storage

Session Storage

IndexedDB

Web SQL

Cookies

http://localhost:8000

Cache

Cache Storage

Application Cache

Filter

Name	Value	Domain	Path	Expires / Max-Age	Size	HTTP	Secure	SameSite
------	-------	--------	------	-------------------	------	------	--------	----------

Console

Network conditions

top

Filter

Default levels

☐ Group similar



# Hello, world!

Thank you for trusting us

These are the cookies you are being given:

- **FOOBAR\_CONSENT:** 1
- **FOOBAR:** 0pioht1i7hclu8mkl4tqr14p3r

Elements

Console

Application

Sources

Network

Performance

Memory

Security

Audits

Adblock Plus

Local Storage

Session Storage

IndexedDB

Web SQL

Cookies

http://localhost:8000

Cache

Cache Storage

Application Cache

Filter

Name	Value	Domain	Path	Expires / Max-Age	Size	HTTP	Secure	SameSite
FOOBAR	0pioht1i7hclu8mkl4tqr14p3r	localhost	/	1969-12-31T23:59:59.000Z	32			
FOOBAR_CONSENT	1	localhost	/	2019-03-01T15:34:04.698Z	15	✓		

Console

Network conditions

top

Filter

Default levels

☐ Group similar



# START SESSIONS ONLY AFTER CONSENT COOKIE IS SET

---

```
<?php
```

```
$consent = false;  
if ([ ] !== $_COOKIE && array_key_exists('FOOBAR_CONSENT', $_COOKIE)) {  
    session_name('FOOBAR');  
    session_start();  
    $consent = true;  
}  
?>
```



# LET USERS CONTROL THIS THROUGH YOUR COOKIE WALL

---

```
<?php
```

```
setcookie('FOOBAR_CONSENT', 1, time() + (60*60*24*356), "", "", FALSE, TRUE);  
header('Location: /sessions.php');
```















# REMOVE THE “DATA”

---











*from views and interfaces*













	First name	Last name	Email Address	Phone number	
	Emmanuel	Bernier	mary.bins@erdman.org	402.631.6451	<a href="#">→ Details</a>
	Amelia	Koelpin	davon11@nitzsche.com	1-285-628-8218	<a href="#">→ Details</a>
	Catalina	Mills	schinner.velva@zieme.com	1-641-503-2660 x46240	<a href="#">→ Details</a>
	Ted	Wolf	loraine80@stracke.com	312-360-2685 x61882	<a href="#">→ Details</a>
	Annabel	Kiehn	cgrimes@sporer.com	731-923-3775 x770	<a href="#">→ Details</a>
	Candice	Mohr	koch.adele@feeney.info	841-957-3664 x32082	<a href="#">→ Details</a>
	Sigurd	Bechtelar	kemmer.murray@ferry.com	1-747-959-8775 x516	<a href="#">→ Details</a>
	Patsy	Altenwerth	oral.weimann@greenholt.org	(960) 424-7589 x72950	<a href="#">→ Details</a>
	Genevieve	Schroeder	collier.miguel@boyer.com	(856) 573-3093 x187	<a href="#">→ Details</a>
	Elta	Toy	tillman.bart@jacobs.com	338-974-7254	<a href="#">→ Details</a>

# What's wrong with this picture?













	First name	Last name	Email Address	Phone number	
	Emmanuel	Bernier	mary.bins@erdman.org	402.631.6451	<a href="#">→ Details</a>
	Amelia	Koelpin	davon11@nitzsche.com	1-285-628-8218	<a href="#">→ Details</a>
	Catalina	Mills	schinner.velva@zieme.com	1-641-503-2660 x46240	<a href="#">→ Details</a>
	Ted	Wolf	loraine80@stracke.com	312-360-2685 x61882	<a href="#">→ Details</a>
	Annabel	Kiehn	cgrimes@sporer.com	731-923-3775 x770	<a href="#">→ Details</a>
	Candice	Mohr	koch.adele@feeney.info	841-957-3664 x32082	<a href="#">→ Details</a>
	Sigurd	Bechtelar	kemmer.murray@ferry.com	1-747-959-8775 x516	<a href="#">→ Details</a>
	Patsy	Altenwerth	oral.weimann@greenholt.org	(960) 424-7589 x72950	<a href="#">→ Details</a>
	Genevieve	Schroeder	collier.miguel@boyer.com	(856) 573-3093 x187	<a href="#">→ Details</a>
	Elta	Toy	tillman.bart@jacobs.com	338-974-7254	<a href="#">→ Details</a>

*Why display full name details?*

	First name	Last name	Email Address	Phone number	
	Emmanuel	Bernier	mary.bins@erdman.org	402.631.6451	<a href="#">→ Details</a>
	Amelia	Koelpin	davon11@nitzsche.com	1-285-628-8218	<a href="#">→ Details</a>
	Catalina	Mills	schinner.velva@zieme.com	1-641-503-2660 x46240	<a href="#">→ Details</a>
	Ted	Wolf	loraine80@stracke.com	312-360-2685 x61882	<a href="#">→ Details</a>
	Annabel	Kiehn	cgrimes@sporer.com	731-923-3775 x770	<a href="#">→ Details</a>
	Candice	Mohr	koch.adele@feeney.info	841-957-3664 x32082	<a href="#">→ Details</a>
	Sigurd	Bechtelar	kemmer.murray@ferry.com	1-747-959-8775 x516	<a href="#">→ Details</a>
	Patsy	Altenwerth	oral.weimann@greenholt.org	(960) 424-7589 x72950	<a href="#">→ Details</a>
	Genevieve	Schroeder	collier.miguel@boyer.com	(856) 573-3093 x187	<a href="#">→ Details</a>
	Elta	Toy	tillman.bart@jacobs.com	338-974-7254	<a href="#">→ Details</a>

*Why display email addresses?*



	First name	Last name	Email Address	Phone number	
	Emmanuel	Bernier	mary.bins@erdman.org	402.631.6451	<a href="#">→ Details</a>
	Amelia	Koelpin	davon11@nitzsche.com	1-285-628-8218	<a href="#">→ Details</a>
	Catalina	Mills	schinner.velva@zieme.com	1-641-503-2660 x46240	<a href="#">→ Details</a>
	Ted	Wolf	loraine80@stracke.com	312-360-2685 x61882	<a href="#">→ Details</a>
	Annabel	Kiehn	cgrimes@sporer.com	731-923-3775 x770	<a href="#">→ Details</a>
	Candice	Mohr	koch.adele@feeney.info	841-957-3664 x32082	<a href="#">→ Details</a>
	Sigurd	Bechtelar	kemmer.murray@ferry.com	1-747-959-8775 x516	<a href="#">→ Details</a>
	Patsy	Altenwerth	oral.weimann@greenholt.org	(960) 424-7589 x72950	<a href="#">→ Details</a>
	Genevieve	Schroeder	collier.miguel@boyer.com	(856) 573-3093 x187	<a href="#">→ Details</a>
	Elta	Toy	tillman.bart@jacobs.com	338-974-7254	<a href="#">→ Details</a>











*Why display phone numbers?*

# REDUCE ACCESS TO DETAILS











---

*If a user has other ways to communicate with your clients, remove the visible display of common data elements like full names, email and shipment addresses and phone numbers.*













First name	Last name	Job title	Company	
 E.	Bernier	Law Enforcement Teacher	<a href="#">Leffler Inc</a>	<a href="#">✉ Email</a> <a href="#">☎ Call</a> <a href="#">➔ Details</a>
 A.	Koelpin	Life Scientists	<a href="#">Nolan, Oberbrunner and Schuppe</a>	<a href="#">✉ Email</a> <a href="#">☎ Call</a> <a href="#">➔ Details</a>
 C.	Mills	Database Manager	<a href="#">Wyman, Hagenes and Shanahan</a>	<a href="#">✉ Email</a> <a href="#">☎ Call</a> <a href="#">➔ Details</a>
 T.	Wolf	Production Planner	<a href="#">Kohler-Mitchell</a>	<a href="#">✉ Email</a> <a href="#">☎ Call</a> <a href="#">➔ Details</a>
 A.	Kiehn	Claims Taker	<a href="#">Gutkowski Ltd</a>	<a href="#">✉ Email</a> <a href="#">☎ Call</a> <a href="#">➔ Details</a>
 C.	Mohr	Multi-Media Artist	<a href="#">Upton, Huel and Howell</a>	<a href="#">✉ Email</a> <a href="#">☎ Call</a> <a href="#">➔ Details</a>
 S.	Bechtelar	Music Arranger and Orchestrator	<a href="#">Heller-Ortiz</a>	<a href="#">✉ Email</a> <a href="#">☎ Call</a> <a href="#">➔ Details</a>
 P.	Altenwerth	Biologist	<a href="#">Volkman-Wilderman</a>	<a href="#">✉ Email</a> <a href="#">☎ Call</a> <a href="#">➔ Details</a>
 G.	Schroeder	Information Systems Manager	<a href="#">Romaguera LLC</a>	<a href="#">✉ Email</a> <a href="#">☎ Call</a> <a href="#">➔ Details</a>
 E.	Toy	Director Of Marketing	<a href="#">Williamson LLC</a>	<a href="#">✉ Email</a> <a href="#">☎ Call</a> <a href="#">➔ Details</a>

Do you see the difference?

First name	Last name	Job title	Company	
 E.	Bernier	Law Enforcement Teacher	<a href="#">Leffler Inc</a>	<a href="#">✉ Email</a> <a href="#">☎ Call</a> <a href="#">➔ Details</a>
 A.	Koelpin	Life Scientists	<a href="#">Nolan, Oberbrunner and Schuppe</a>	<a href="#">✉ Email</a> <a href="#">☎ Call</a> <a href="#">➔ Details</a>
 C.	Mills	Database Manager	<a href="#">Wyman, Hagenes and Shanahan</a>	<a href="#">✉ Email</a> <a href="#">☎ Call</a> <a href="#">➔ Details</a>
 T.	Wolf	Production Planner	<a href="#">Kohler-Mitchell</a>	<a href="#">✉ Email</a> <a href="#">☎ Call</a> <a href="#">➔ Details</a>
 A.	Kiehn	Claims Taker	<a href="#">Gutkowski Ltd</a>	<a href="#">✉ Email</a> <a href="#">☎ Call</a> <a href="#">➔ Details</a>
 C.	Mohr	Multi-Media Artist	<a href="#">Upton, Huel and Howell</a>	<a href="#">✉ Email</a> <a href="#">☎ Call</a> <a href="#">➔ Details</a>
 S.	Bechtelar	Music Arranger and Orchestrator	<a href="#">Heller-Ortiz</a>	<a href="#">✉ Email</a> <a href="#">☎ Call</a> <a href="#">➔ Details</a>
 P.	Altenwerth	Biologist	<a href="#">Volkman-Wilderman</a>	<a href="#">✉ Email</a> <a href="#">☎ Call</a> <a href="#">➔ Details</a>
 G.	Schroeder	Information Systems Manager	<a href="#">Romaguera LLC</a>	<a href="#">✉ Email</a> <a href="#">☎ Call</a> <a href="#">➔ Details</a>
 E.	Toy	Director Of Marketing	<a href="#">Williamson LLC</a>	<a href="#">✉ Email</a> <a href="#">☎ Call</a> <a href="#">➔ Details</a>

*Not full name display*



First name	Last name	Job title	Company	
 E.	Bernier	Law Enforcement Teacher	<a href="#">Leffler Inc</a>	<a href="#">✉ Email</a> <a href="#">☎ Call</a> <a href="#">➔ Details</a>
 A.	Koelpin	Life Scientists	<a href="#">Nolan, Oberbrunner and Schuppe</a>	<a href="#">✉ Email</a> <a href="#">☎ Call</a> <a href="#">➔ Details</a>
 C.	Mills	Database Manager	<a href="#">Wyman, Hagenes and Shanahan</a>	<a href="#">✉ Email</a> <a href="#">☎ Call</a> <a href="#">➔ Details</a>
 T.	Wolf	Production Planner	<a href="#">Kohler-Mitchell</a>	<a href="#">✉ Email</a> <a href="#">☎ Call</a> <a href="#">➔ Details</a>
 A.	Kiehn	Claims Taker	<a href="#">Gutkowski Ltd</a>	<a href="#">✉ Email</a> <a href="#">☎ Call</a> <a href="#">➔ Details</a>
 C.	Mohr	Multi-Media Artist	<a href="#">Upton, Huel and Howell</a>	<a href="#">✉ Email</a> <a href="#">☎ Call</a> <a href="#">➔ Details</a>
 S.	Bechtelar	Music Arranger and Orchestrator	<a href="#">Heller-Ortiz</a>	<a href="#">✉ Email</a> <a href="#">☎ Call</a> <a href="#">➔ Details</a>
 P.	Altenwerth	Biologist	<a href="#">Volkman-Wilderman</a>	<a href="#">✉ Email</a> <a href="#">☎ Call</a> <a href="#">➔ Details</a>
 G.	Schroeder	Information Systems Manager	<a href="#">Romaguera LLC</a>	<a href="#">✉ Email</a> <a href="#">☎ Call</a> <a href="#">➔ Details</a>
 E.	Toy	Director Of Marketing	<a href="#">Williamson LLC</a>	<a href="#">✉ Email</a> <a href="#">☎ Call</a> <a href="#">➔ Details</a>

*Integrated communication functionality*

## Send message to Ted Wolf

**Ted Wolf**

Production Planner | Kohler-Mitchell

### Message

Send messageCancel

Hey Ted,

Works for me! Looking forward meeting you and your colleagues next Tuesday at 10am at your office.

Michelangelo

**You** wrote:

2017-04-25 17:12:53

Hi Michelangelo,

Thank you for your phone call earlier, I've discussed your proposal with our CEO and we would like to hear more about how your business can help us becoming GDPR compliant. Can we make an appointment for next week Tuesday 10am at our offices? I'm also inviting our HR manager to this meeting as well. Does this work for you?

Best regards,  
Ted

**Ted** wrote:

2017-04-25 16:41:10

Hey hi Ted,



# SAME FUNCTIONALITY, BUT KEEPS DATA HIDDEN

---

- Prevents accidentally exposing email and phone numbers (e.g. during a call)
- Hides details from end-user, but functionality is still provided
  - Sending out an email uses build-in mail client
  - Making calls uses a phone middleware used in the company
- Gives clear audit trail on who accessed what

Date	User	Action	IP
2017-04-24 15:44:22	<a href="#">michelangelo</a>	Added note to contact <a href="#">#434</a>	10.92.16.31
2017-04-24 14:22:44	<a href="#">friedel</a>	Updated deal <a href="#">#1234</a> to status <b>won</b>	10.92.16.31
2017-04-24 12:41:21	<a href="#">michelangelo</a>	Called contact <a href="#">#992</a>	10.92.16.31
2017-04-24 10:39:29	<a href="#">friedel</a>	Send mail to contact <a href="#">#1543</a>	10.92.16.18
2017-04-24 09:16:02	<a href="#">friedel</a>	Created new contact <a href="#">#1543</a>	10.92.16.18
2017-04-24 08:23:11	<a href="#">michelangelo</a>	Added note to deal <a href="#">#1234</a>	10.92.16.31
2017-04-24 08:21:01	<a href="#">friedel</a>	Successfully authenticated into the app	10.92.16.18
2017-04-24 08:19:38	<a href="#">michelangelo</a>	Created deal <a href="#">#1234</a>	10.92.16.31
2017-04-24 08:06:51	<a href="#">michelangelo</a>	Successfully authenticated into the app	10.92.16.31
2017-04-23 15:44:22	<a href="#">michelangelo</a>	Added note to contact <a href="#">#434</a>	10.92.16.31
2017-04-23 14:22:44	<a href="#">friedel</a>	Updated deal <a href="#">#1234</a> to status <b>won</b>	10.92.16.31
2017-04-23 12:41:21	<a href="#">michelangelo</a>	Called contact <a href="#">#992</a>	10.92.16.31
2017-04-23 10:39:29	<a href="#">friedel</a>	Send mail to contact <a href="#">#1543</a>	10.92.16.18
2017-04-23 09:16:02	<a href="#">friedel</a>	Created new contact <a href="#">#1543</a>	10.92.16.18
2017-04-23 08:23:11	<a href="#">michelangelo</a>	Added note to deal <a href="#">#1234</a>	10.92.16.31
2017-04-23 08:21:01	<a href="#">friedel</a>	Successfully authenticated into the app	10.92.16.18
2017-04-23 08:19:38	<a href="#">michelangelo</a>	Created deal <a href="#">#1234</a>	10.92.16.31
2017-04-23 08:06:51	<a href="#">michelangelo</a>	Successfully authenticated into the app	10.92.16.31
2017-04-22 15:44:22	<a href="#">michelangelo</a>	Added note to contact <a href="#">#434</a>	10.92.16.31
2017-04-22 14:22:44	<a href="#">friedel</a>	Updated deal <a href="#">#1234</a> to status <b>won</b>	10.92.16.31
2017-04-22 12:41:21	<a href="#">michelangelo</a>	Called contact <a href="#">#992</a>	10.92.16.31



# NOT 100% PROTECTION, BUT...

---

- We remove the personal one-on-one communication with customers
- We add better access management on customer communication
- Full audit trail now possible as communication stays in-application
- Less chance for data loss as contact details are kept away from users

# BLOCKCHAIN

---

*Immutable, verifiable ledger for all transactions*





# AUTOMATE

---

*Anonymisation and Data Leakage Prevention*



# REGULAR EXPRESSIONS

---

```
cat server.log | sed -r 's/([0-9]+\.)\.[0-9]+\.  
[0-9]+\.)\.[0-9]+)\1.xxx.xxx.\4/g' -
```

```
52.xxx.xxx.233 - - [01/Sep/2017:00:32:31 +0300] "GET / HTTP/1.1" 200 1
52.xxx.xxx.226 - - [01/Sep/2017:00:32:47 +0300] "GET / HTTP/1.1" 200 1
79.xxx.xxx.186 - - [01/Sep/2017:00:37:27 +0300] "POST /wp-cron.php?do=
192.xxx.xxx.40 - - [01/Sep/2017:00:37:27 +0300] "HEAD / HTTP/1.1" 200
13.xxx.xxx.102 - - [01/Sep/2017:00:38:08 +0300] "GET / HTTP/1.1" 200 1
45.xxx.xxx.76 - - [01/Sep/2017:00:38:14 +0300] "GET / HTTP/1.1" 200 17
52.xxx.xxx.12 - - [01/Sep/2017:00:38:37 +0300] "GET / HTTP/1.1" 200 17
52.xxx.xxx.96 - - [01/Sep/2017:00:38:39 +0300] "GET / HTTP/1.1" 200 17
79.xxx.xxx.186 - - [01/Sep/2017:00:39:16 +0300] "POST /wp-cron.php?do=
45.xxx.xxx.155 - - [01/Sep/2017:00:39:16 +0300] "GET / HTTP/1.1" 200 1
52.xxx.xxx.226 - - [01/Sep/2017:00:39:30 +0300] "GET / HTTP/1.1" 200 1
79.xxx.xxx.186 - - [01/Sep/2017:00:39:36 +0300] "POST /wp-cron.php?do=
52.xxx.xxx.233 - - [01/Sep/2017:00:39:36 +0300] "GET / HTTP/1.1" 200 1
52.xxx.xxx.227 - - [01/Sep/2017:00:40:07 +0300] "GET / HTTP/1.1" 200 1
52.xxx.xxx.53 - - [01/Sep/2017:00:40:26 +0300] "GET / HTTP/1.1" 200 17
52.xxx.xxx.66 - - [01/Sep/2017:00:40:40 +0300] "GET / HTTP/1.1" 200 17
45.xxx.xxx.106 - - [01/Sep/2017:00:41:23 +0300] "GET / HTTP/1.1" 200 1
176.xxx.xxx.65 - - [01/Sep/2017:00:41:25 +0300] "GET / HTTP/1.1" 200 1
54.xxx.xxx.165 - - [01/Sep/2017:00:41:26 +0300] "GET / HTTP/1.1" 200 1
52.xxx.xxx.138 - - [01/Sep/2017:00:41:39 +0300] "GET / HTTP/1.1" 200 1
13.xxx.xxx.88 - - [01/Sep/2017:00:42:06 +0300] "GET / HTTP/1.1" 200 17
13.xxx.xxx.37 - - [01/Sep/2017:00:42:11 +0300] "GET / HTTP/1.1" 200 17
207.xxx.xxx.148 - - [01/Sep/2017:00:42:11 +0300] "GET /page/10/ HTTP/1
192.xxx.xxx.216 - - [01/Sep/2017:00:42:19 +0300] "GET / HTTP/1.1" 200
192.xxx.xxx.40 - - [01/Sep/2017:00:42:24 +0300] "HEAD / HTTP/1.1" 200
52.xxx.xxx.27 - - [01/Sep/2017:00:42:30 +0300] "GET / HTTP/1.1" 200 17
79.xxx.xxx.186 - - [01/Sep/2017:00:42:33 +0300] "GET /wp-content/uploa
79.xxx.xxx.186 - - [01/Sep/2017:00:42:33 +0300] "GET /wp-content/uploa
79.xxx.xxx.186 - - [01/Sep/2017:00:42:33 +0300] "GET /wp-content/uploa
79.xxx.xxx.186 - - [01/Sep/2017:00:42:33 +0300] "GET /wp-content/uploa
79.xxx.xxx.186 - - [01/Sep/2017:00:42:33 +0300] "GET /wp-content/uploa
66.xxx.xxx.41 - - [01/Sep/2017:00:42:33 +0300] "GET /tag/conference/fe
81.xxx.xxx.243 - - [01/Sep/2017:00:43:56 +0300] "GET /wp-content/uploa
81.xxx.xxx.243 - - [01/Sep/2017:00:43:56 +0300] "GET /wp-content/uploa
81.xxx.xxx.243 - - [01/Sep/2017:00:43:56 +0300] "GET /wp-content/uploa
81.xxx.xxx.243 - - [01/Sep/2017:00:43:56 +0300] "GET /wp-content/uploa
81.xxx.xxx.243 - - [01/Sep/2017:00:43:56 +0300] "GET /wp-content/uploa
79.xxx.xxx.186 - - [01/Sep/2017:00:43:57 +0300] "POST /wp-cron.php?do=
74.xxx.xxx.34 - - [01/Sep/2017:00:43:57 +0300] "GET /feed HTTP/1.1" 30
81.xxx.xxx.243 - - [01/Sep/2017:00:43:58 +0300] "GET /favicon.ico HTTP
79.xxx.xxx.186 - - [01/Sep/2017:00:44:58 +0300] "POST /wp-cron.php?do=
52.xxx.xxx.223 - - [01/Sep/2017:00:44:58 +0300] "HEAD /feed HTTP/1.1"
63.xxx.xxx.244 - - [01/Sep/2017:00:45:00 +0300] "HEAD / HTTP/1.1" 200
192.xxx.xxx.40 - - [01/Sep/2017:00:47:26 +0300] "HEAD / HTTP/1.1" 200
```



# DATA LOSS PROTECTION (DLP)

---

*Prevent leakage on company level*



# EXAMPLES OF DLP

Office 365

Security & Compliance

Home

Alerts

Permissions

Classifications

Data loss prevention

Policy

Device management

Device security policies

App permissions

Data governance

Home > Data loss prevention

Use data loss prevention (DLP) policies to docs isn't shared with the wrong people. L

Create a policy

Refresh

Name

Google Data Loss Prevention Demo

1 Welcome to the Data Loss Prevention Demo.

2

3 Type or paste some text here to test the DLP API. Findings appear below.

4

5 For example, strings like this one produce a PHONE\_NUMBER finding:

6 "Please call me. My phone number is (555) 253-0000."

7

8 Customizing:

9 To choose classification categories, click "Info types" on the right.

10

11 Certainty:

12 Findings are ranked on a certainty scale of 0 (least certain) to 1 (most

13 certain). The raw certainty number is provided for each finding:

14 Low (0.0 to 0.499)

15 Medium (0.5 to 0.799)

16 High (0.8 to 1)

17

18 Low scores may introduce noise in the results, especially when a particular

19 string matches multiple detectors. To limit the findings to high scores,

20 select "High certainty" on the right.

21

Options

☒ Welcome text

☐ High certainty

INFO TYPES: 50/60

Privacy  
Terms of Service  
Send Feedback

Findings

Type	Certainty	String	Line:Char	Offset (bytes)		
PHONE_NUMBER	High (1)	(555) 253-0000	6:41	224	👍	👎
CREDIT_CARD_NUMBER	High (1)	4012-8888-8888-1881	24:25	807	👍	👎
US_HEALTHCARE_NPI	High (1)	1245319639	25:35	861	👍	👎
EMAIL_ADDRESS	High (0.9)	foo@example.com	23:20	757	👍	👎
DOMAIN_NAME	High (0.9)	example.com	23:24	771	👍	👎
US_DRIVERS_LICENSE_NUMBER	High (0.9)	AC333991	26:23	894	👍	👎
CANADA_BC_PHN	Low (0.2)	1245319639	25:35	861	👍	👎
UK_TAXPAYER_REFERENCE	Low (0.05)	1245319639	25:35	861	👍	👎

DLP TEST

[Home](#)[HTTP Post](#)[HTTPS Post](#)[FTP Test](#)[Sample Data](#)[FAQ](#)[Contact](#)

What is dlptest.com used for?

DLPTes.com is a Data Loss Prevention (DLP) testing resource that focuses on testing to make sure your DLP software is working correctly. If DLP has been installed correctly and the DLP policies have been built correctly, this website can be used to demonstrate your data is being protected. Data Loss Prevention is typically broken into three vectors called Data-In-Use (DIU), Data-At-Rest (DAR), and Data-In-Motion (DIM). DLPTes.com currently has features to test Data-In-Use and Data-In-Motion.

What is Data-In-Use?

Data-In-Use also known as Endpoint Protection requires installing an endpoint Agent on the user computers. The Endpoint Agents should be installed on laptops, desktops, and virtual desktops such as Citrix VDI. Once the Endpoint Agent has been installed the DLP software can be set up to monitor different channels. Most vendors support USB transfers, CD/DVD burning, moving data from Network Shares, monitoring web browsers (IE, Chrome, Firefox), FTP transfers, and cloud storage as supported channels for monitoring.

What is Data-In-Motion?

Data-In-Motion is the ability to monitor traffic on the network including but not limited to HTTP, HTTPS, FTP, SFTP, SSH, Telnet, SMTP, POP3, IMAP4, and more.





# EMAIL MARKETING

---

*My contact list is the lifeline of our business!!!*



# CONTACT DATA

---

*Opt-in , always*





# NOT OPT-IN

---

*/dev/null is the place to be*





KEEP  
CALM  
AND  
LET'S  
RECAP

## RECAP

---

- Users give data in trust: respect that
- Ensure private data is kept to a minimum and removed from view
- Protect your data by anonymization and remove from view interfaces
- Know that security is not enough: if you don't have it, it can't be stolen!



## GDPR Deadline

00	02	03	04	14	34
Years	Months	Days	Hours	Minutes	Seconds



# QUESTIONS?

---







PROFESSIONAL PHP SERVICES

**Michelangelo van Dam**  
*Zend Certified Engineer*

**Consulting**

**Automation**

**Training**

[contact@in2it.be](mailto:contact@in2it.be) - [www.in2it.be](http://www.in2it.be) -  [in2itvof](https://twitter.com/in2itvof) -  [in2itvof](https://facebook.com/in2itvof)