# Employee Privacy Is Now A Corporate Imperative

DeleteMe

**For everyone in your organization, privacy is too important to be treated as a personal matter. Instead, the security of every individual's personal information, from the boardroom to the ground floor, needs to be a corporate concern.**

With information privacy under continuous attack, employees are living with a growing privacy deficit. Wherever they go online, everyone in your organization leaves a trail of information that is being captured, aggregated, analyzed, profiled, stored, traded, and sold — without their knowledge or permission.

For your organization, the personal identity trail created by employees has another downside — greater corporate risk.

**44%** of data breaches were caused by employees who inadvertently exposed sensitive information to hackers or data thieves.[1]

**20%** of adults have experienced online harassment that often continues offline.[2]

Organizations spend an average of **$4M** annually dealing with phishing attacks.[4]

**83%** of 7,000 global info security professionals responded to phishing attacks on the network. Attacks show increasing sophistication, using employee PII for authenticity.[3]

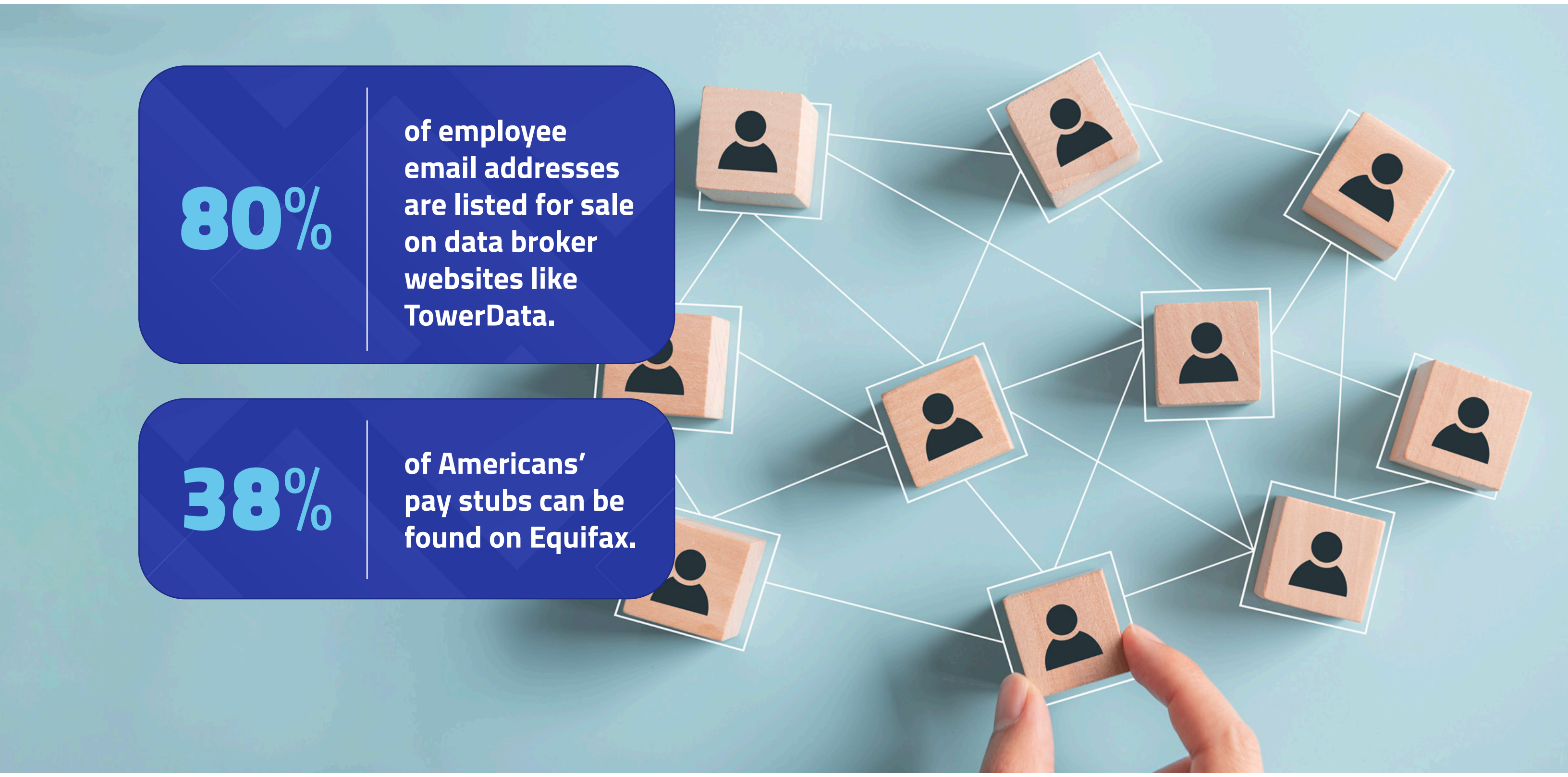
[1] Forrester Research
[2] HONR Network
[3] Proofpoint
[4] Ponemon Institute

# Shrinking the growing personal data footprint employees leave behind is becoming more difficult.

## Today, more than 630 tracking technologies are being used to gather a wide range of information on individuals:

- Names and birthdays
- Mailing addresses (current, previous, and forwarding)
- Phone numbers (personal and corporate)
- Email addresses (personal and corporate)
- Medical information
- Estimated education and income level
- Financial information
- Associations, memberships, religious and political affiliations
- Marriage and divorce records
- Licenses (automotive and professional)
- Civil and criminal court records
- Homeownership, mortgage holders/value

Although aggregating personal information is legal, the accessibility of employees' private information creates real risks for organizations. As well as employee safety and satisfaction, business cybersecurity and organizational productivity both depend on keeping employee information private. When privacy is compromised, employees and businesses alike suffer.



**80%** of employee email addresses are listed for sale on data broker websites like TowerData.

**38%** of Americans' pay stubs can be found on Equifax.

# How **Privacy Helps** Your Organization

Personal information falling into third parties' hands is dangerous for your organization, yet this is often realized too late.

### Employee privacy should underpin your organization's security posture.

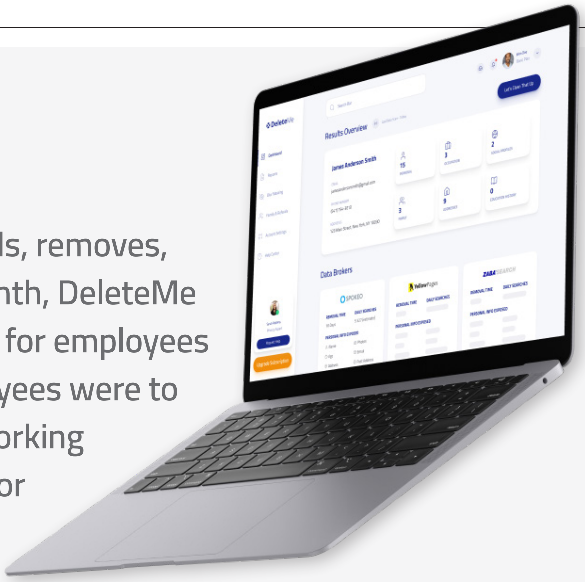
Implementing layers of security across the network perimeter, access, data, applications, and devices won't keep your organization safe from hackers and other bad actors. Today, exposed employee personal information is too often the weakest link in the cybersecurity chain.

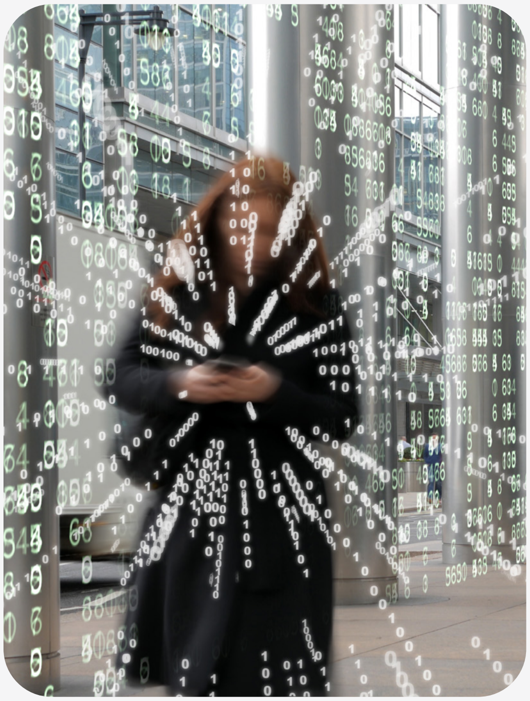
### Privacy protection is a powerful tool for recruiting and engaging employees.

Employees want to protect their personal information, but they often don't know how or lack the right tools to do so. When HR helps employees keep their personal information private, workplace privacy can become an attractive benefit.

# How **DeleteMe** Helps

DeleteMe is the leading proactive privacy service that finds, removes, and monitors for exposed personal information. Each month, DeleteMe removes over 25,000 personal listings and search results for employees in organizations spanning every business sector. If employees were to do this themselves, they would have to invest up to 76 working days — plus additional days every three months to monitor for new data sources listing their personal information.





## 92%

surveyed believed that voluntary benefits such as personal data protection would be important for their employees in the coming years.

## **Bolsters** Cybersecurity

Phishing scams built off leaked personal information are unrecognizable to 97% of employees. To take one real-world example, an executive expressing interest in cricket on Facebook opened a door for hackers to deploy ransomware.

## Keeps Executives & Employees **Safe**

According to a study by the Ontic Center For Protective Intelligence, 69% of executives have witnessed a dramatic increase in physical threat activity. Protecting employees and their families from harassment necessitates personal data removal.

## **Mitigates** Reputational Damage

When private information is exposed in a doxxing attack, it can damage the reputation of both employees and the organization they work for.

## **Increases** Productivity & Satisfaction

Leaked personal information not only helps feed the barrage of marketing robocalls and junk email that employees face every day but can also lead to identity theft and cyberstalking.

An employee experiencing a severe misuse of their personal information can expect to spend an average of 165 hours resolving the issue. Unsurprisingly, BenefitsPro named personal identity protection as one of the top voluntary benefits that employees want.

# How **DeleteMe** Works

## 1 **Employees, Executives**, and **Board Members Complete Web-Based Sign Up** (3-10 Minutes to Complete)

After individuals submit information for opt-out and removal, DeleteMe's Privacy Advisors get to work. No further action from you or your employees is required.

## 2 **DeleteMe Searches** for **Exposed Personal Information**

DeleteMe Privacy Advisors use the DeleteMe tech platform to scan, match, and find unwanted instances of employees' corporate and personal information online. DeleteMe can search for thousands of iterations of each board member, employee, and executive's personal and corporate data. We find newly-exposed information that is published on new sources on an ongoing basis, including personal data that is:

- Listed for sale by data brokers.
- Highly ranked in Google for common phishing and personal info search queries.
- Publicly-searchable in other online and offline databases.

## 3 **DeleteMe Does** the **Removal Work**

As soon as we find personal information, we start removing it. To do this, DeleteMe sends custom opt-out and removal requests to all matching data brokers. Removal at the source can take from hours to four weeks, depending on the source provider's compliance responsiveness.

- DeleteMe removes employee data from over 50 sources and executive data from more than 100 sources, including stubborn listings that rank highly on Google.

## 4 **You Get Continuous, Detailed Privacy Reporting** in a **Simple PDF Format**

Board members, employees, and executives receive regular detailed personalized DeleteMe privacy reports. We show you where each piece of personal information was exposed and how we are removing it. Ongoing reporting at various frequencies (monthly to quarterly) is automatic. These reports are sent out by email, but both employees and the corporate administrator of the Employee Privacy Program can also access them through their DeleteMe Dashboard.

## 5 **DeleteMe Provides** Continuous Privacy Protection **All Year**

DeleteMe never stops working. We continually monitor data brokers to ensure employee and executive personal and corporate information is not exposed without approval and easily accessible to malicious actors who may use this information for phishing attacks and/or harassment purposes. Continuous removal is critical because new, unregulated sources appear every day and existing data brokers constantly try to re-list and re-expose personal data. DeleteMe adds new data brokers and sources of personal information exposure all year to our service — and these are added FREE of charge to your annual subscription. Should you have any questions, an assigned DeleteMe Privacy Advisor is available to contact as part of the subscription.

# A Proactive Approach for Removing Unwanted Employee Personal Information from the Public Domain

In operation since 2009, with over 25,000,000 opt-outs successfully completed, DeleteMe is the leader in Employee Privacy Programs trusted by hundreds of Fortune 500 companies. Offered by Abine, DeleteMe is today's leading employee privacy information identification, removal, and monitoring service for board members, executives, and employees; reducing cyber threats, social engineering/phishing attacks, doxxing/online harassment, physical threats, robocalls, and spam/unwanted marketing.

## For Its Corporate Clients, DeleteMe Provides:

- On-going scanning and proactive removal of employee personal information across new sources of exposure (online & offline).
- Regular reporting that clearly shows exposed data and removal status for each employee covered by the service.
- Dedicated privacy advisors to work with employees and executives.
- Dedicated customer support for your organization.

**Profitable, VC-Backed** privacy company founded in

**2009**

**Customers Include Over**

**30%** of Fortune 100

**Successfully Completed Over** **25M** opt-outs

with a **4.75/5** verified review score