eBOOK

3 Overlooked Data Privacy Considerations

THE C-SUITE'S MORAL, ETHICAL, AND LEGAL RESPONSIBILITY TO PROTECT PII

ABSOLUTE®

SUMMARY

Data privacy is something that affects us all.

People want to interact with organizations that take our data privacy seriously. As a result, taking a stance on data privacy is not just morally and ethically right — it makes good business sense.

This eBook explores what personal privacy means in a 'dematerialized' world and draws attention to three aspects of data protection that often go overlooked.

CONTENTS

INTRODUCTION: THE "DEMATERIALIZATION" OF SOCIETY 04

DATA RESIDENCY 07

ORCHESTRATION OF CONTROLS 08

CONTINUOUS MONITORING 08

NEXT STEPS 09

INTRODUCTION

THE "DEMATERIALIZATION" OF SOCIETY

Look around your home today and compare it with a home in the 1980s or 90s. What's missing? An answering machine, Rolodex, calendar, alarm clock, road maps, vinyl records, VHS tapes, cassettes, CDs, and DVDs, the list goes on. Each of those material goods has been replaced by our smartphones. Digital has "dematerialized" our world — even our money has been digitized, for the most part. It's safe to say we're much less dependent on physical stuff.

CASH TRANSACTIONS ARE TRUMPED BY DIGITAL TRANSACTIONS

Digital has also dematerialized people. A person is a person because of the data that exists about them — our digital selves. We have become a collection of individual pieces of data made up of Personally Identifiable Information, or PII.

32%

of US transactions are in cash.[1]

34%

of UK transactions are in cash but UK debit cards transactions overtook cash for the first time in 2018.[2]

25%

of Canadian transactions are in cash.[3]

[1] Federal Reserve Bank. 2015. The State of Cash: Preliminary Findings from the 2015 Diary of Consumer Payment Choice

[2] Kollewe, Julia, 2018. UK debit cards transactions overtake cash for the first time, The Guardian

[3] La Rose, Lauren. 2016. More Canadians choosing credit cards, mobile payments over cash, study says, Globe and Mail.

PERSONAL PRIVACY IN A DEMATERIALIZED WORLD

When all our personal data is digital, privacy becomes a much bigger issue, with many more stakeholders. With all the progress society has made during our digital transformation, we somehow managed to sacrifice our personal privacy along the way. We shifted from moving physical material that makes up a person's identity around in space to moving bits and bytes around in the cloud — and somehow this shift made the data seem less valuable for a while.

THREE ATTITUDES TO THE DEMATERIALIZATION OF PERSONAL DATA

"JUST STAY OFFLINE."
1.
"MY DATA WILL BE USED (AND MISUSED)—IT'S NO BIG DEAL."
2.
"WAIT A SECOND — THAT DATA *IS* WHO I AM!"
3.

Let's talk about these three attitudes. In the case of the first, staying offline is not realistic today. Digital transformation has occurred, and it's very difficult to participate in society while remaining offline. Business, government, banking, school, research, and social interactions are now happening in the digital town square.

The second, devil-may-care attitude, is irresponsible. Would it be a "big deal" if their identity was stolen and their credit rating was destroyed? It's safe to assume that it would be.

Most of us are represented by the third — we care about our data. Especially today, when there is a global crisis in trust. The 2019 Edelman Trust Barometer found that 15 of 26 markets around the world lie in distruster territory (or the third attitude referenced above). [4]

There have been too many stories in the news about organizations and institutions for all the wrong reasons — negligence and loss of personal data, cybersecurity breaches, inadvertent misuse of data by a third party, and so on.

[4] Edelman. 2019. Edelman Trust Barometer: Global Report

As a result, governments around the world are stepping up to the challenge of protecting the privacy of the individual with strict regulations (backed by law) that govern the use and misuse of digital data, and shift power back to the individual.

NEW AND UPDATED REGULATIONS TO PROTECT OUR DIGITAL SELVES

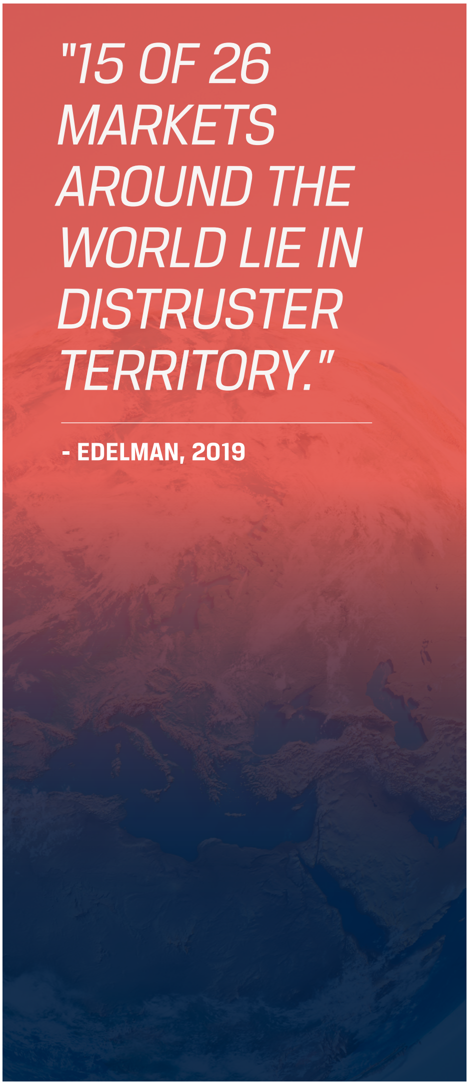
Sweeping regulations, such as the EU General Data Protection Regulation (GDPR), are prompting regulators around the world to implement compatible standards and, in some cases, start levying their own fines.

Most recently, the California Consumer Privacy Act (CCPA) as well as Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) were introduced. Both have been heavily influenced by GDPR and give people more control over the personal information that is being collected about them.

THE C-SUITE HAS AN ETHICAL RESPONSIBILITY TO PROTECT PII

There are several reasons why organizations should do everything in their power to protect PII. Firstly, it's the law. Data breaches can be bad for business both in terms of regulatory fines and loss of business due to class-action suits. Not to mention the subsequent reputation damage.

Secondly — and more importantly — there's an ethical responsibility: it's the right thing to do. And the public expects organizational leaders to take charge — 76% of those surveyed in the 2019 Edelman Trust Barometer believe that CEOs should take the lead on change, rather than waiting for the government to impose it.



"15 OF 26 MARKETS AROUND THE WORLD LIE IN DISTRUSTER TERRITORY."

- EDELMAN, 2019

The C-suite has a responsibility to take an active role in ensuring data security and privacy controls are in place — failure to do so puts innocent people at risk and could potentially be the digital world equivalent of reckless endangerment.

There are three simple aspects of data privacy that often go overlooked:

DATA RESIDENCY

Are you certain you know where your data is hiding?

ORCHESTRATION OF CONTROLS

How are your security controls policed?

CONTINUOUS MONITORING

Can you be sure data is not residing in the wrong place and, if it is, that security controls are in place to protect it?

DATA RESIDENCY

Your organization is full of sensitive data. You need it to fuel your business. It helps you make decisions, predict customer churn, target your marketing campaigns, and so on. Generally speaking, PII is accessed only via approved business applications.

Your employees would never export data from Salesforce.com and save it on their laptop. They'd never save an Excel spreadsheet containing PHI to their hard drive. They'd certainly never sync a proposal containing proprietary company information to Dropbox.

The problem is that your employees would do all of the above. And they do. Your sensitive data is sitting out there on more endpoints than you think. You need the equivalent of Google for your endpoint data — a lexicographical crawler for PHI and PII data that can alert you to any unauthorized data hiding out there on endpoint devices. Unless you have that, you simply won't be able to track all the places where the data resides.

One laptop is stolen every 53 seconds.[5] What happens when one of those laptops belongs to your organization? Results from a recent Forrester security survey found that 39 percent of breaches can be traced back to the endpoint (24 percent caused by employee misuse and 15 percent caused by lost or missing devices).[6] Without the ability to know what data resides on a device, you've no idea if you've exposed your customers to a data breach risk.

> *"ONE LAPTOP IS STOLEN EVERY 53 SECONDS."*
>
> **-FORBES**

[5] Olenski, S. 2017. Is The Data On Your Business' Digital Devices Safe? Forbes, December 8, 2017

[6] Forrester, 2018. Forrester Analytics Global Business Technographics Security Survey

ORCHESTRATION OF CONTROLS

There is no shortage of security controls, whether they be native in the operating system or third-party applications like antivirus, antimalware, encryption, or other endpoint detection and response (EDR) solutions. These controls help ensure that the place that data resides is a secure one.

The problem organizations face is ensuring that the third-party controls remain in place and are functioning at all times. Native controls can help with this, giving organizations the ability to pull information from the controls and push actions to the device if they are not operating as they should or if the user of the device is acting suspiciously.

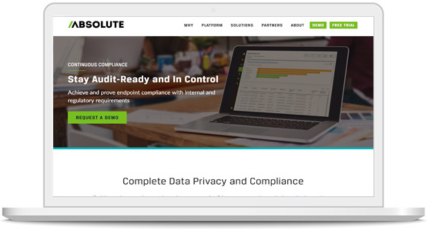
This is particularly important in a breach scenario. For example, if a company laptop is stolen from the trunk of your employee's car and you know that the laptop contains PHI, without visibility into that device, you have no way to prove that encryption was in place and functioning and that no data was accessed post-incident. In this scenario, you would have to assume that the data was breached and follow HIPAA's breach notification rules.

With the right visibility in place, you can categorically prove that security controls were in place on a device, that no data was accessed, and that the device has been locked down and is no longer a threat.

CONTINUOUS MONITORING

Annual auditing is only valid on the day the audit takes place. Can you be sure on any day in between audits that data is not residing in the wrong place and, if it is, that security controls are in place to protect it? Without continuous monitoring, you'll never be able to keep track of all the data copies that exist on all your devices. This can leave you in hot water when the regulators come knocking.

Say, for example, that you have a customer who resides in Nice, France. They notify your company that they want to be erased from your records. Under GDPR, you have to find every stitch of their data that is saved in your organization and erase it. You can pull them from your data lakes — that's the easy part — but shards of their data will still exist out there on numerous endpoints, leaving you exposed to sanctions under GDPR.



CONTINUOUS COMPLIANCE

Stay Audit-Ready and In Control

Achieve and prove endpoint compliance with internal and regulatory requirements

Complete Data Privacy and Compliance

To learn more about how Absolute can help you stop a cybersecurity threat from becoming a data breach, visit: absolute.com/compliance

In this scenario, you need the ability to reverse your gaze, looking outwards rather than inwards, and surgically delete their data elements from your endpoints. Without this ability, you'll be helpless to identify the millions of Achilles heels that exist on endpoints and that will violate the regulations and ethical code of digital data protection.

NEXT STEPS

Data privacy affects all of us. As the world becomes increasingly dematerialized, we can expect everyone to take a greater interest in their digital selves. The organizations that act now to build data privacy into their company's mission statement will be the ones that retain customer trust. Follow these simple steps to get started...

1 **Build your data ethics code**
From the CEO to the administrative team, everyone in your organization should be trained to treat data privacy with the reverence it deserves. Your data ethics code should be intentional, public, and comprehensive enough to satisfy even the most austere regulators.

2 **Perfect your security foundation**
Use native security to ensure complete visibility and control over all endpoints. These solutions are built into the firmware of devices and can't be tampered with. They should be the foundation on which you build the rest of your security controls. With this foundation in place, you'll know where your data resides, have the ability or orchestrate controls seamlessly, and be confident that you can monitor the data and controls continuously.

3 **Implement a cybersecurity framework**
A cybersecurity framework (CSF) can help you get your house in order, formalize your security disciplines, and scale your security operations by prioritizing doing the right things in the right way. Many organizations are adopting the model recommended by the National Institute of Standards and Technology (NIST). The NIST Cybersecurity Framework[7] can help you evaluate your security posture by implementing functions to ensure data security and business sustainability.

[7] National Institute of Standards and Technology (NIST). 2018. The NIST cybersecurity framework

Is your organization compliant? Evaluate your risk with a free assessment highlighting potential areas of exposure.

GET IT NOW

ABOUT ABSOLUTE

Absolute empowers more than 12,000 customers worldwide to protect devices, data, applications and users against theft or attack — both on and off the corporate network. With the industry's only tamper-proof endpoint visibility and control solution, Absolute allows IT to enforce asset management, security hygiene, and data compliance for today's remote digital workforces. Patented Absolute Persistence™ is embedded in the firmware of Dell, HP, Lenovo, and most leading manufacturers' devices for vendor-agnostic coverage, tamper-proof resilience, and ease of deployment. See how it works at **www.absolute.com** and follow us at **@absolutecorp**.

EMAIL:
sales@absolute.com

SALES:
absolute.com/request-info

PHONE:
North America: 1-877-660-2289
EMEA: +44-118-902-2000

WEBSITE:
absolute.com

© 2019 Absolute Software Corporation. All rights reserved. Absolute and Persistence are registered trademarks of Absolute Software Corporation. For patent information, visit www.absolute.com/patents. Data_Privacy-EB-022819.