

# Where Law and Tech Will Collide in 2020

**Angelique Carson, Editor**

**Rita Heimes, GC & Chief Privacy Officer**

**Cathy Scerbo, VP, Chief Information Officer**

**RSA<sup>®</sup>**  
Conference

# The International Association of Privacy Professionals

The Mission of the **IAPP** is to Define, Promote and Improve the Privacy Profession Globally.



# Key Principles of Privacy.



Minimization



User Control



Purpose Limitation



Security

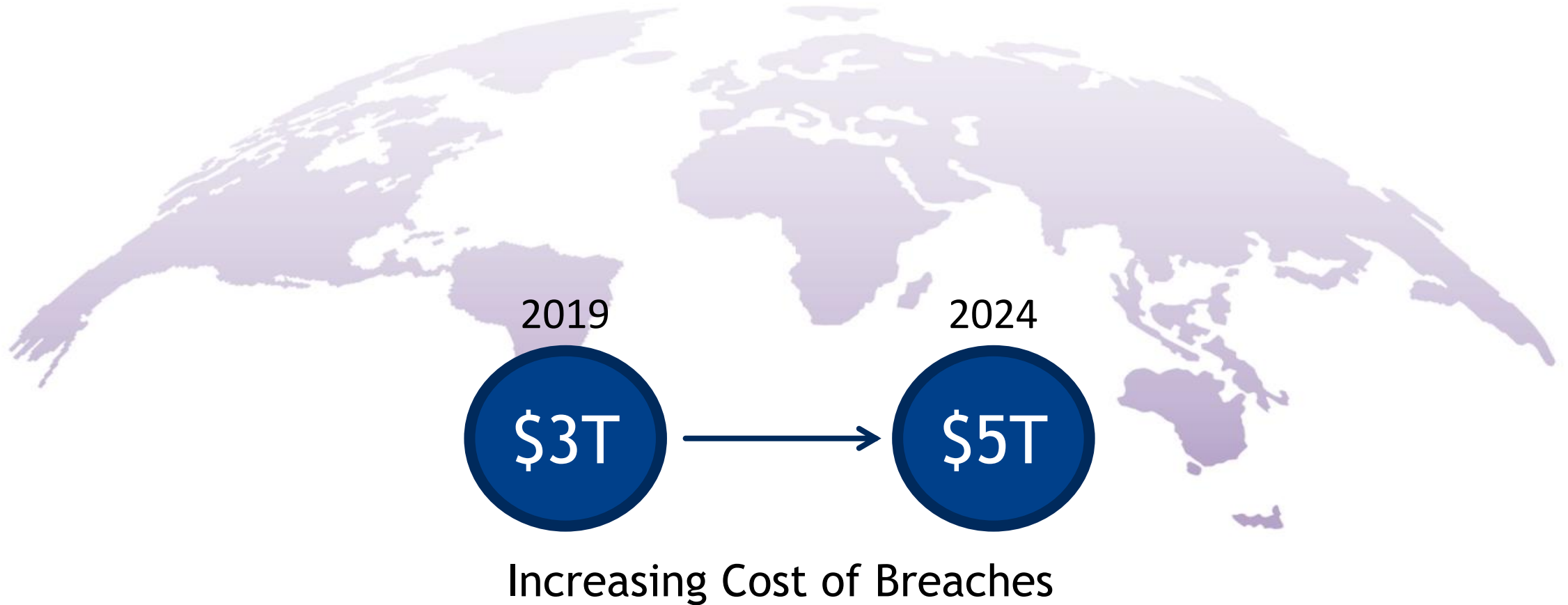


Notice and Consent

Laws are being defined to address the use of data.



# Globally, the laws are becoming more stringent and enforcement is ramping up





---

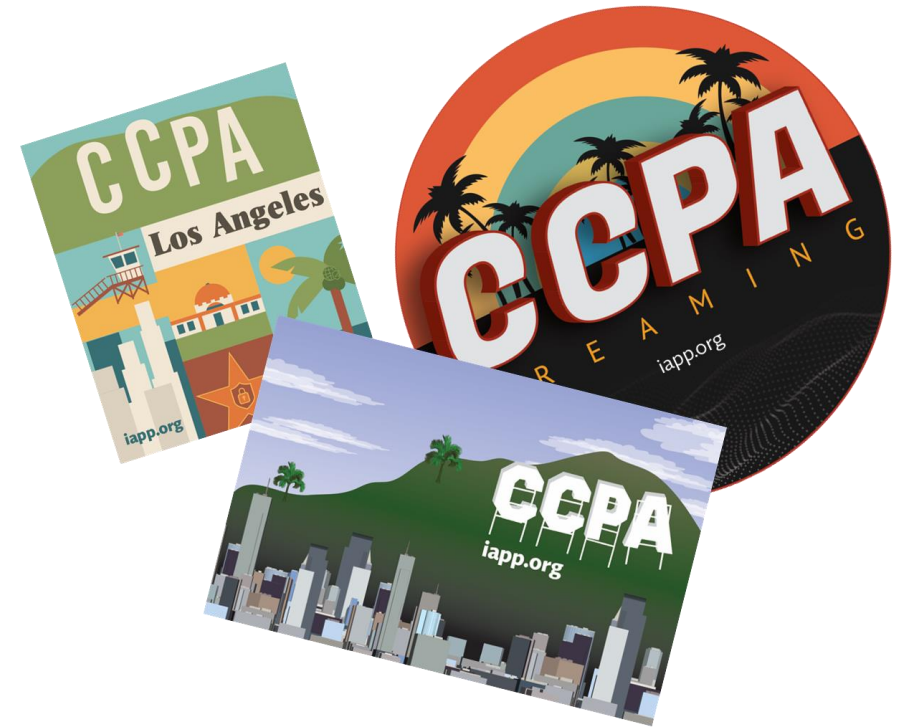
Right to correct  
inaccuracies

---

Right to be forgotten

---

Right to place restrictions  
on the processing



---

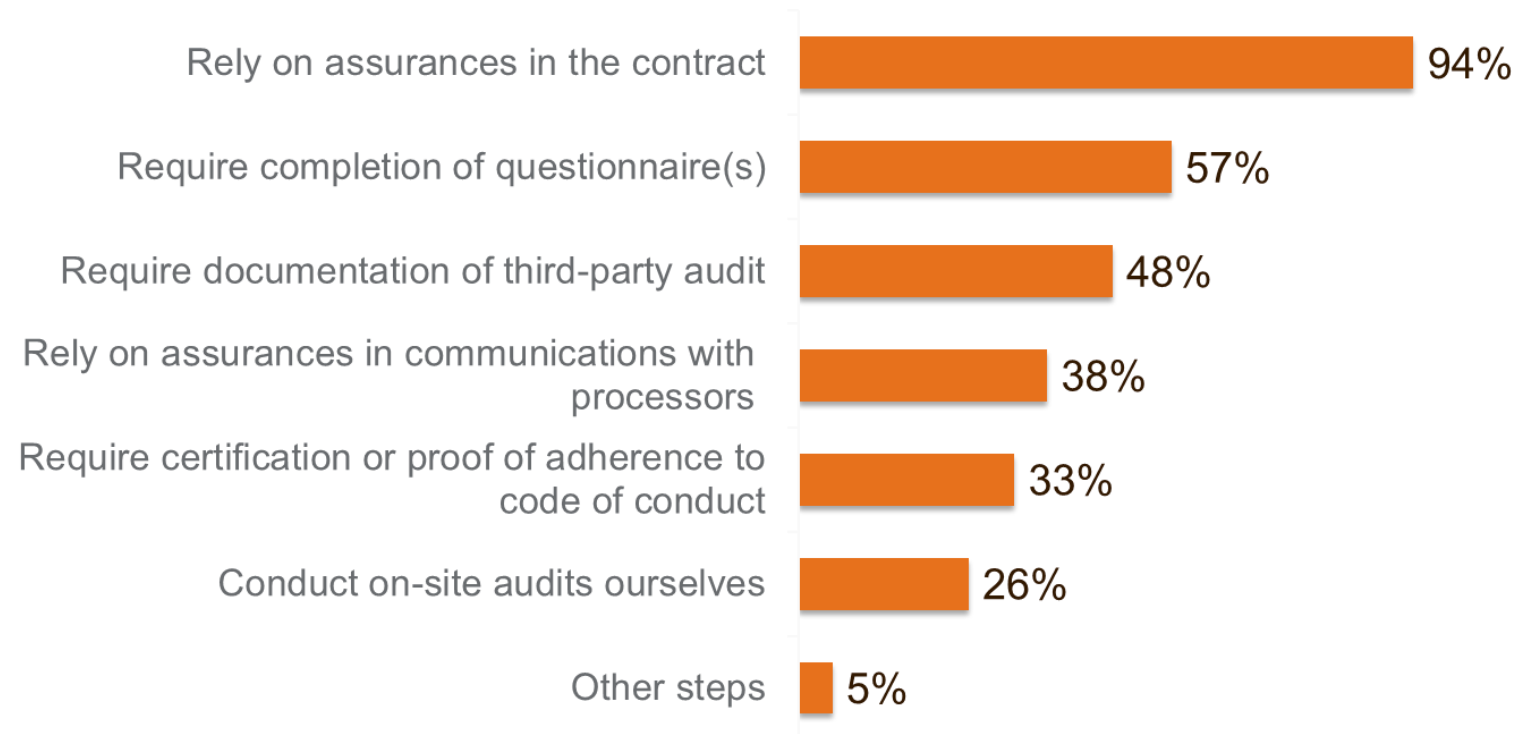
Right to instruct not to  
sell to a 3rd party

---

Contracts are most commonly used to ensure compliance

## Steps Taken to Ensure Processor Responsibilities

(Base: use other companies for processing)

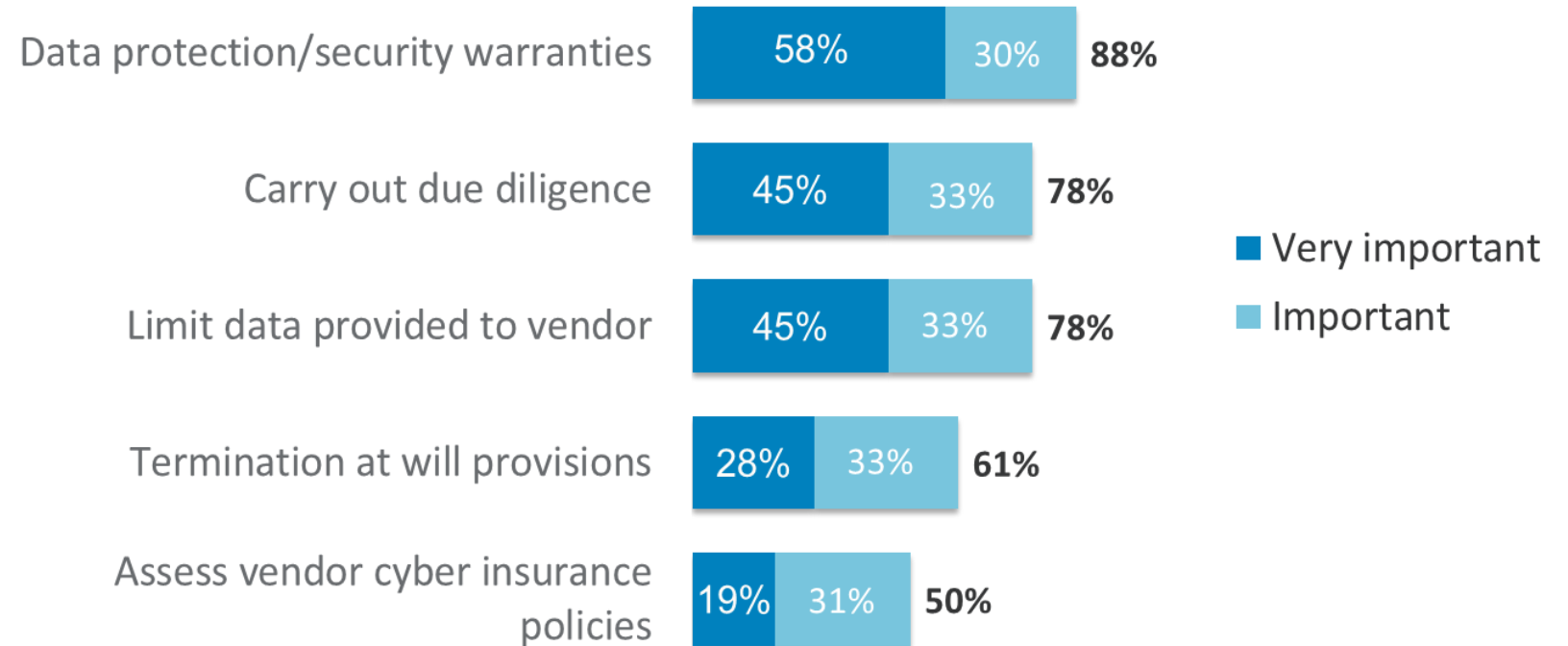


H8: What steps do you take to ensure your processors are doing what they've committed to doing?

When privacy pros are choosing a processor, contractual warranties are their top consideration

## Importance of Processor Considerations

(Base: use other companies for processing)



K4-K8: In selecting data processors, how important is it to your company to...



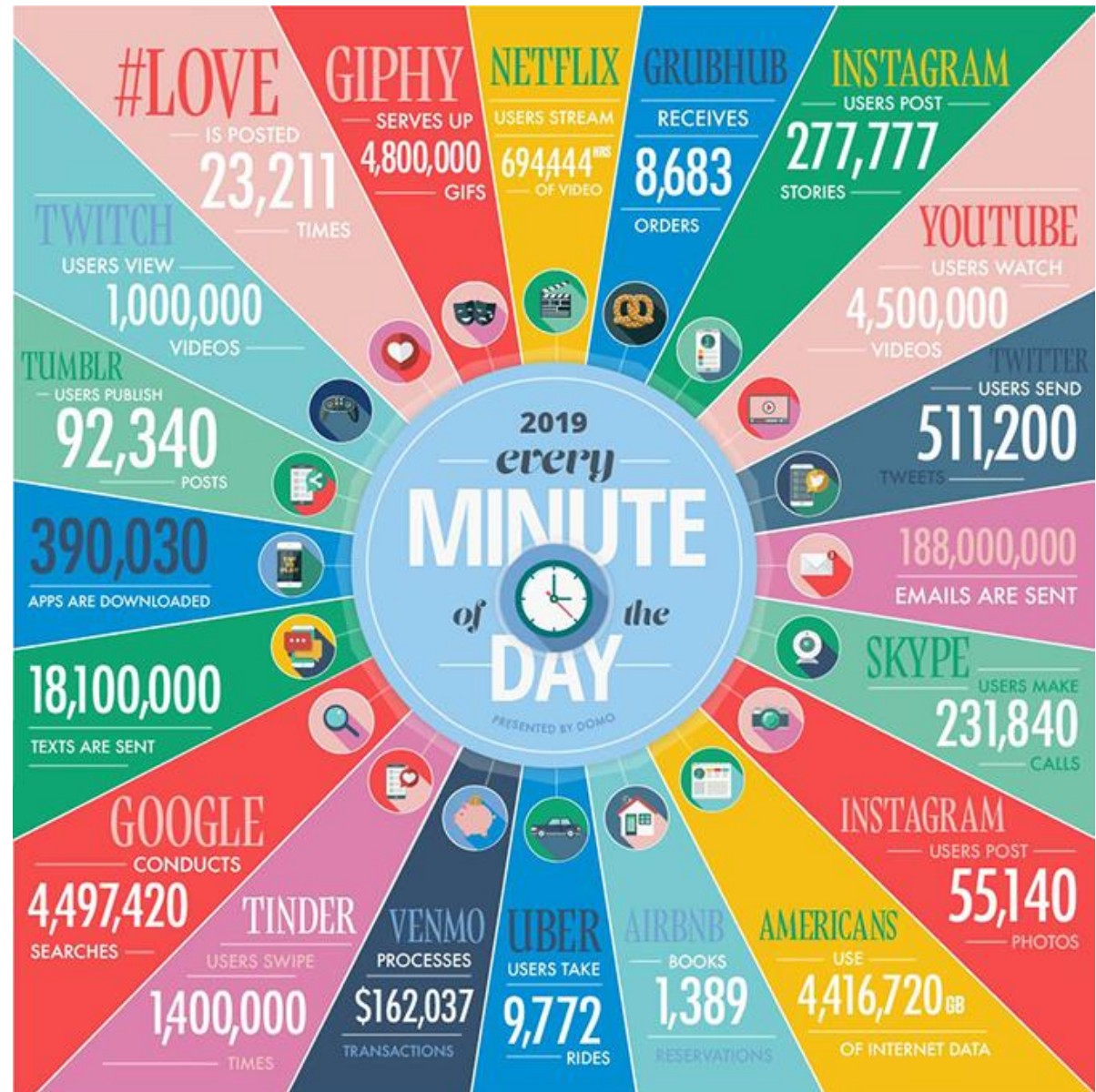


There are 31 billion  
connected devices In  
the world today.

By 2025, that number  
is projected to be 75  
billion.



Every minute we voluntarily create and share data.





“Privacy is more important than ever in today’s digital age”

Walter G. Copan

Under Secretary of Commerce for  
Standards and Technology,

NIST Director

# Laws *require* compliance with the principles of **Privacy by Design**.

- changes plan, design, build, test and maintain applications
- Affects the way we vet and integrate Third Party Software

## 7 PRINCIPLES OF PRIVACY BY DESIGN



### PROACTIVE, NOT REACTIVE, PREVENTATIVE, NOT REMEDIAL

The Privacy by Design approach is characterised by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. PbD does not wait for privacy risks to materialise, nor does it offer remedies for resolving privacy infractions once they have occurred – it aims to prevent them from occurring. In short, Privacy by Design comes before-the-fact, not after.



### FULL FUNCTIONALITY – POSITIVE-SUM, NOT ZERO-SUM

Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum “win-win” manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. Privacy by Design avoids the pretense of false dichotomies, such as privacy vs. security, demonstrating that it is possible to have both.



### PRIVACY AS THE DEFAULT SETTING

Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy – it is built into the system, by default.



### END-TO-END SECURITY

Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved – strong security measures are essential to privacy, from start to finish. This ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion. Thus, Privacy by Design ensures cradle to grave, secure lifecycle management of information, end-to-end.



### PRIVACY EMBEDDED INTO THE DESIGN

Privacy by Design is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.



### VISIBILITY AND TRANSPARENCY

Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.

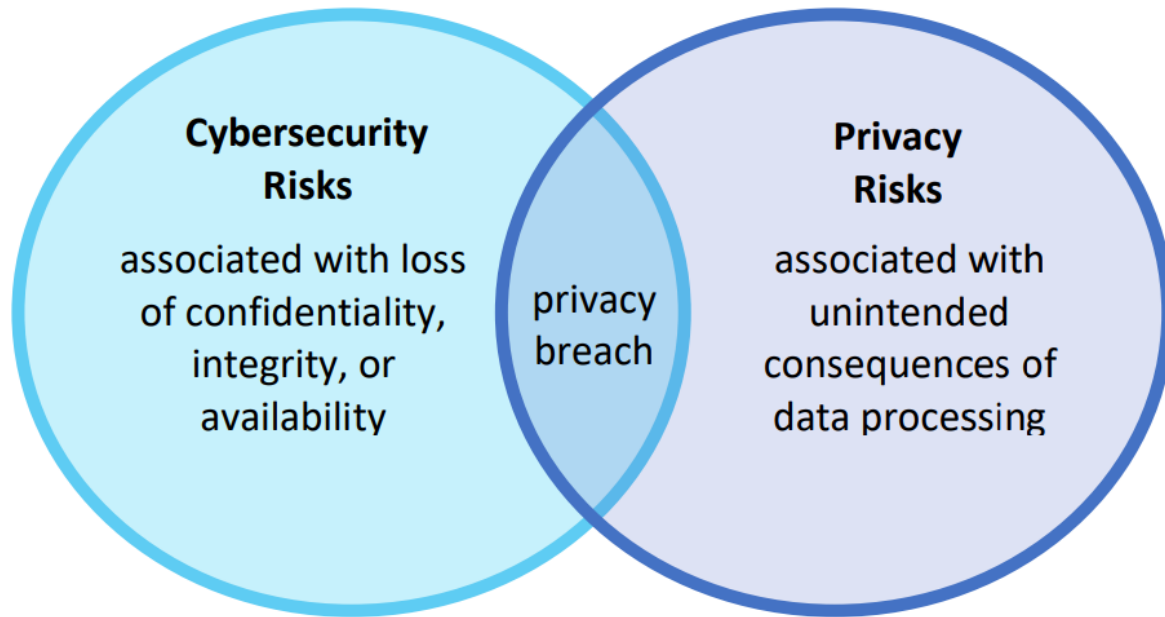


### RESPECT FOR USER PRIVACY

Above all, Privacy by Design requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.

Helping small businesses work towards Data Protection Compliance and deliver on their Web Application Goals

[www.ServeIT.com](http://www.ServeIT.com)



## Emergent Privacy Guidance

- Collaborative effort launched September 2018
- Version 1.0 released January 16<sup>th</sup> 2020
- Security is key in protection of privacy

The NIST Security and Privacy Frameworks are tightly aligned.

## CYBERSECURITY RISKS

IDENTIFY  
PROTECT  
DETECT  
RESPOND  
RECOVER

## PRIVACY BREACH RISKS

PROTECT - P  
DETECT  
RESPOND  
RECOVER

## PRIVACY RISKS

IDENTIFY - P  
GOVERN - P  
CONTROL - P  
COMMUNICATE - P



Security is about protection and availability. It requires rules & restrictions.

Privacy is about content, context and usage. It requires **ethics** and **trust**.



Partnership of  
Legal and Tech  
is critical!

