



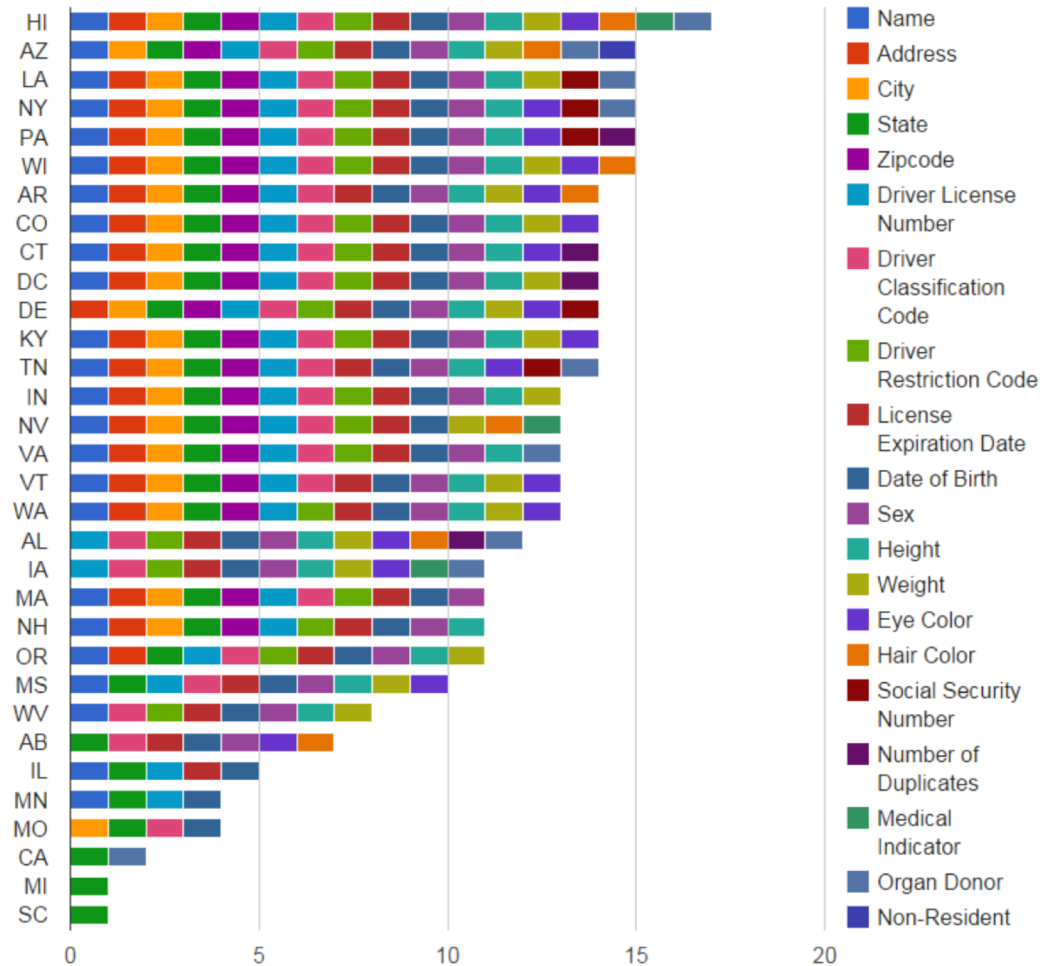
# To Trust of Not To Trust

What Every Startup Needs To Know About Privacy and Cybersecurity

CONNECTS Seminar at Carnegie Mellon: OCTOBER 14, 2020

John Funge, DataTribe

Drivers License Attributes on 2D Barcode by State



Source: <http://mantascode.com/us-drivers-license-barcode-attributes-by-state/>



# Biggest Data Breaches of the 21<sup>st</sup> Century

---

Year	Company	Lost Records (million)
2018	Marriott	500
2017	Equifax	143
2016	Adult Friend Finder	412
2015	Anthem	79
2014	Ebay	145
2014	JP Morgan Chase	76
2014	Home Depot	56
2013	Yahoo	3000
2013	Target Stores	110
2013	Adobe	38
2012	OPM	22
2011	Sony Playstation Net	77
2011	RSA Security	40
2008	Heartland Payment Sys	134
2006	TJX Companies	94



Source: <https://www.csoononline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html>

# 22 Million Affected by OPM Hack, Officials Say

The extent of the hack has finally been revealed.





“Mark Zuckerberg declared in 2010 that privacy is no longer a “social norm,” but bought the four houses abutting his Palo Alto home to help ensure his own privacy.”

Schneier, Bruce. *Data and Goliath*

“I believe there's an opportunity to set a new standard for private communication platforms...”

Mark Zuckerberg, *A Privacy-focused Vision for Social Media*, March 2019



“When we approach designing products for the home we focus on three key attributes

- ... must be easy to use
- ... work better together
- ... **be secure and protect your privacy”**

Tim Cook, *Apple Launch Event*, October 13, 2020

“It takes 20 years to build a reputation  
and five minutes to ruin it.”

Warren Buffett



# What We'll Talk About

---

- Big Picture
- Few Startup Axioms
- Privacy
- Security
- Questions



# Big Picture







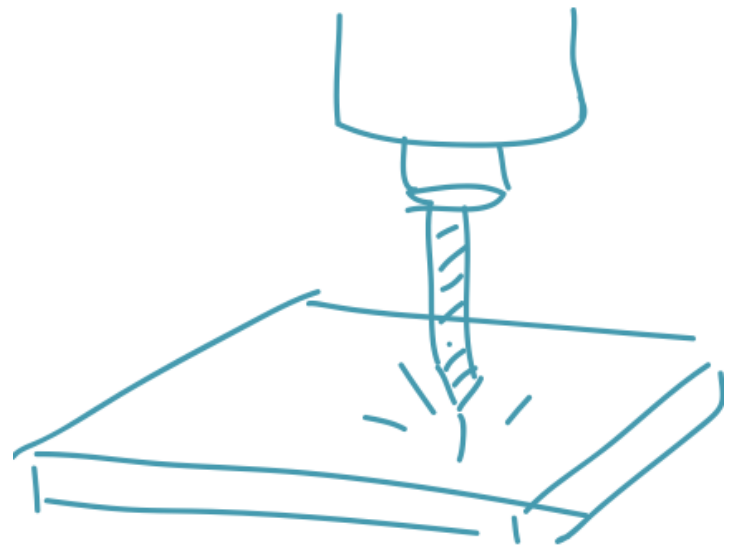
“Privacy doesn’t just depend on agency;  
Being able to achieve privacy is and  
expression *of* agency.”

Danah Boyd quoted in *Data and Goliath* by Bruce Schneier

So, how does this apply to startups?



# Axiom 1: Focus



## Axiom 2: Stage Appropriateness

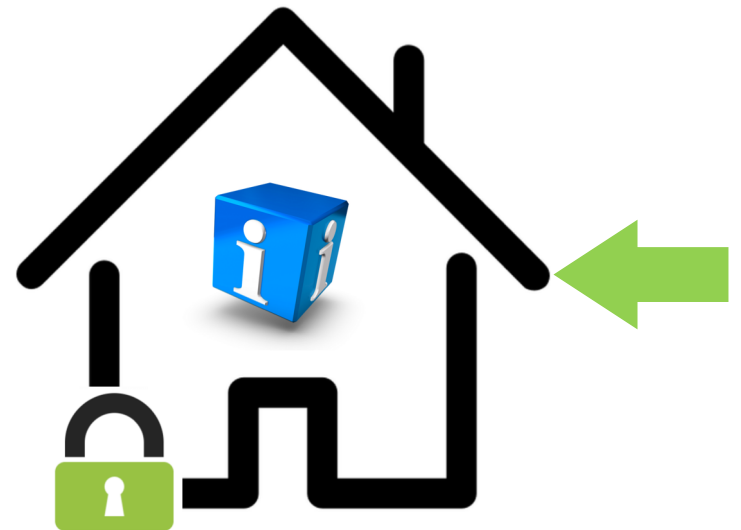


## **Axiom 3:** Find trustworthy trail guides early





# Privacy



# Context

---

- Ever Increasing Digitalization of Life
- Cloud Computing → Democratizing Big Data
- GDPR & CCPA
- AI
- No System is 100% Secure



# Regulations and Trends

---

- There Are Many, It's Sort of a Mess
- Some Key Regulations To Be Aware Of
  - State-level Data Breach Laws
  - General Data Protection Regulation (GDPR)
  - Fair Credit Reporting Act (FCRA)
  - Gramm-Leach-Bliley
  - Can Spam Act
  - Telephone Consumer Protection Act
  - Children's Online Privacy Protection Act (COPPA)
  - Health Insurance Portability and Accountability Act (HIPPA)
  - Federal Election Commission
- Trends
  - National "GDPR-like" Regulation Coming to U.S.
  - California Consumer Privacy Act (CCPA)





# Making Sense of It All

---

- Minimize what you collect
- Handle sensitive data with care
- Carefully evaluate privacy trade-offs
- Diligently protect



# Key Concepts In CCPA

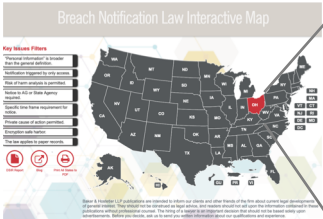
---

- Right to access
- Right to deletion
- Right to knowing if sold, and for what purpose
- Right to opt out







# “Toxic Data” & Data Breach Laws



**BakerHostetler**  
**Ohio**

Ohio Rev. Code Ann. §§ 1347.12 (state agencies), 1349.19 (persons and businesses), 1349.191–192 (2007)

  
Download



**Personal Information (i.e., “Personal Identifying Information”)**

An individual's first name or first initial with last name with one of the following identifiers:

1. Social Security number.
2. Driver's license or identification card number.
3. Account number, credit or debit card number, in combination with and linked to any required security or access code, or password that would permit access to an individual's financial account.

**Persons Covered**

Any person, including any business that is conducted in Ohio and that owns, licenses or maintains computerized data that includes personal information.

Any state agency or agency of a political subdivision.

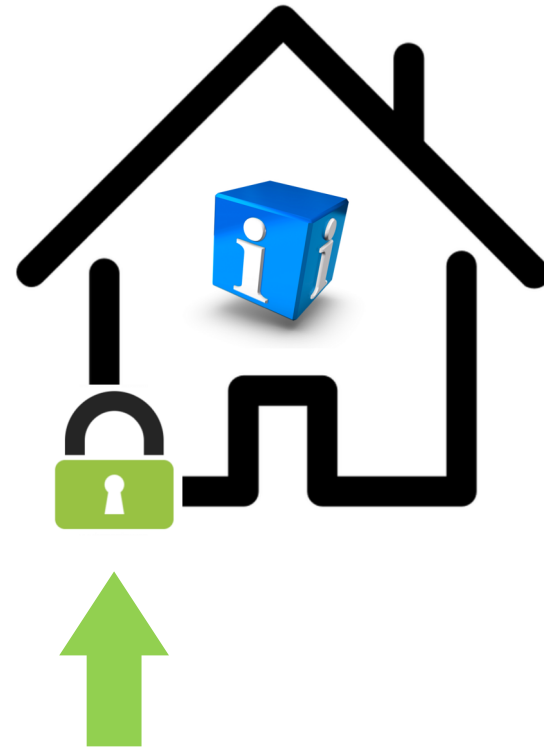
**Encryption/Notification Trigger**

If the data is encrypted, redacted or altered by any method or technology in such a



<https://www.bakerlaw.com/BreachNotificationLawMap>

# Security



## v2.5

## Application Security

WAF & Application Security

[illegible]

## Mobile Security

appdome  BETTER

## IoT

## IoT Devices \_\_\_\_\_

AGARI AREA 1 ASTROD  
BARCO CISCO CLEARSWIFT CYBONE  
EDGEWAVE FIREEYE FORCEPOINT  
FORTINET GFWA INKY  
IRONSCALES MALGUARD MCAFEE MICROSOFT  
MIMECAST PHISHLABS PROOFPOINT QEEXO SOFTWARE  
SONICWALL SOPHOS SPAMHAUS SYMANTEC  
TREND MICRO TRUSTWAVE CODE SECURE  
VOTIRO WEBROOT WICR

## Blockchain

100

CORVUS Deloitte  
 leidos NVG  
 BLACK ARMOUR Chain  
 KRAKEL edge  
 guardtime IDEE Manifold Nulid  
 remme ShoCard vchain xage  
 Ethernity Emailage Ethoca Ever Compliant FICO feedzai  
 Iovation Kount MagicCube MAXIMIZE NetQuadrant  
 simility socure TokenID ThreatMatrix UNIKEN VeriSign

# A Simple Way of Breaking It Down

---

	Offense	Defense
Nation-State	✓	✓
Companies & Criminals	Criminals	Companies
Kids in the Basement	✓	--



Biggest Cyber Trend in 2020...



# Massive Pivot to Remote Work

---





# General Guidelines

---

- Focus on doing the basics well
- Invest where there is risk



# Top 5 Checklist

From Harvard Belfer Center Cybersecurity Campaign Playbook

---

1. Establish a culture of security awareness
2. Use the cloud
3. Use two-factor authentication
4. Encrypted messaging for sensitive comm.
5. Plan and prepare



Source: <https://www.belfercenter.org/cyberplaybook>

Improving your security **is a process.**  
You can take control.  
**Don't just throw your hands up.**



# Essential Cyber Hygiene

---

- “Drive Defensively”
  - Train and remind team members of best practices
  - Don’t use email for sensitive comm.
  - Maintain a vigilant posture clicking links in emails etc.
  - Don’t plug unknown external media into your devices
  - Avoid public WIFI, don’t use for sensitive comm.
  - Be attentive to physical security
- Authentication Practices
  - Two-factor authentication
  - Complex passwords & don’t reuse passwords
  - Password managers
  - Always change default passwords on hardware devices – devices
  - Limit access privileges to just those that need them



# Essential Cyber Hygiene (cont.)

---

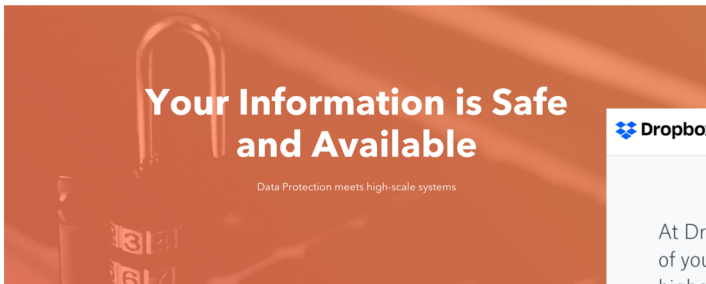
- **Devices and Network**
  - Know your network, audit devices
  - Use an anti-virus
  - Patch and update systems regularly
  - VPN
  - Network segmentation and isolate sensitive systems
  - Get outside audit and pen testing (not early stage, later)
- **Data Protection**
  - Manage and reduce data – reduce attack surface
  - Encryption
  - Make backups
- **Plans & Policy**
  - Ensure you have an effective off-boarding process – policy
  - Create a response plan



## Other Things to Keep in Mind



# Third Party Risk



## Your Information is Safe and Available

Data Protection meets high-scale systems

Our products and services are transforming the sales and marketing industries with the inbound revolution, but the backbone of our success is providing a safe and trustworthy place for marketing and sales data. Protecting your data is our obsession.



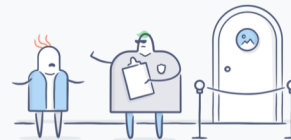
See our plans

At Dropbox, the security of your data is our highest priority

See why millions of people and organizations trust us with their most important work.

Protect your account

Visit the Business Trust Guide



Try free

Buy now



Join your team | Login

## Security at Atlassian

Security is built into the fabric of our Cloud products, infrastructure, and processes, so you can rest assured that your data is safeguarded.

All security practices



### Cloud product security

Security is built into the fabric of our Cloud products. We employ numerous controls to safeguard your data including encryption in transit across our cloud services, external vulnerability research such as our Bug Bounty program, and more.



### Security operations and best practices

Our dedicated security team approaches security holistically with a common controls framework. Security threats are prevented using our Atlassian Trust Management System (ATMS), secure





# Customers & Partners May Hold You Accountable

---

- **Limitation of Liability. EXCEPT WITH RESPECT TO CLAIMS OF INDEMNITY, BREACH OF CONFIDENTIALITY, BREACH OF DATA SECURITY OBLIGATIONS, AND ARISING FROM A DATA INCIDENT (AS SET FORTH IN SECTION XX),** IN NO EVENT SHALL EITHER PARTY BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS/REPUTATIONAL HARM, REVENUE, DATA, OR USE, INCURRED BY OTHER PARTY OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. **EXCEPT WITH RESPECT TO CLAIMS OF INDEMNITY, BREACH OF CONFIDENTIALITY, BREACH OF DATA SECURITY OBLIGATIONS, AND ARISING FROM A DATA INCIDENT (AS SET FORTH IN SECTION XX),** TOTAL LIABILITY FOR A SERVICE IS LIMITED IN ALL CASES AND IN THE AGGREGATE TO THE AMOUNT OF FEES ACTUALLY PAID BY COMPANY FOR THE CORRESPONDING SERVICE DURING THE TWELVE (12) MONTHS PRECEDING THE DATE OF THE EVENT THAT IS THE BASIS FOR THE FIRST CLAIM.



Source: <https://www.winston.com/images/content/1/2/v2/124339/Negotiating-Contractual-Limitations-of-Liability-Provisions-PDF.pdf>

# Be Vigilant of Open Source Tools You Use



**Top 10**

<https://owasp.org/www-project-top-ten>



# Frameworks to Know About

---

- Just to know about...
  - For when your startup scales... not for early-stage
- NIST
  - <https://www.nist.gov/cyberframework>
- System and Organization Controls (SOC)
  - Part of SSAE 16 by American Institute of CPAs
  - <https://www.aicpa.org/soc>



# Cyber Risk Insurance



# Staying Up to Date

---

the  
**cyberwire**

STORIES

PODCASTS

BRIEFINGS

PRO ▾

EVENTS

GLOSSARY

ABOUT ▾

## Audio

---



## Email

---



“Complexity is the worst enemy of security...”

Schneier, Bruce. *Data and Goliath*

“We will bankrupt ourselves in the vain search of absolute security.”

Dwight D. Eisenhower





# Thank You

John Funge

DataTribe

[john.funge@datatribe.com](mailto:john.funge@datatribe.com)

