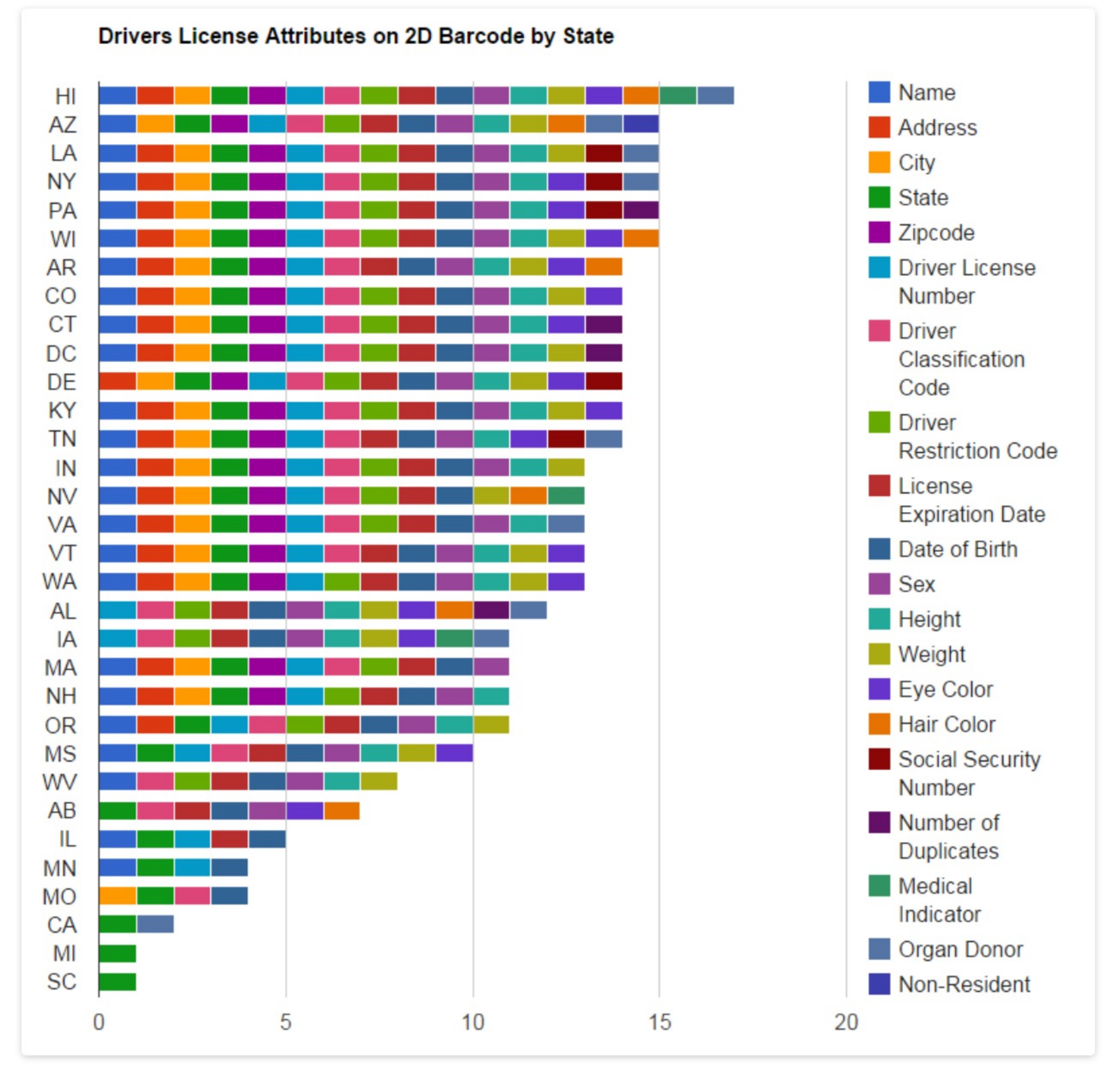
To Trust or Not To Trust

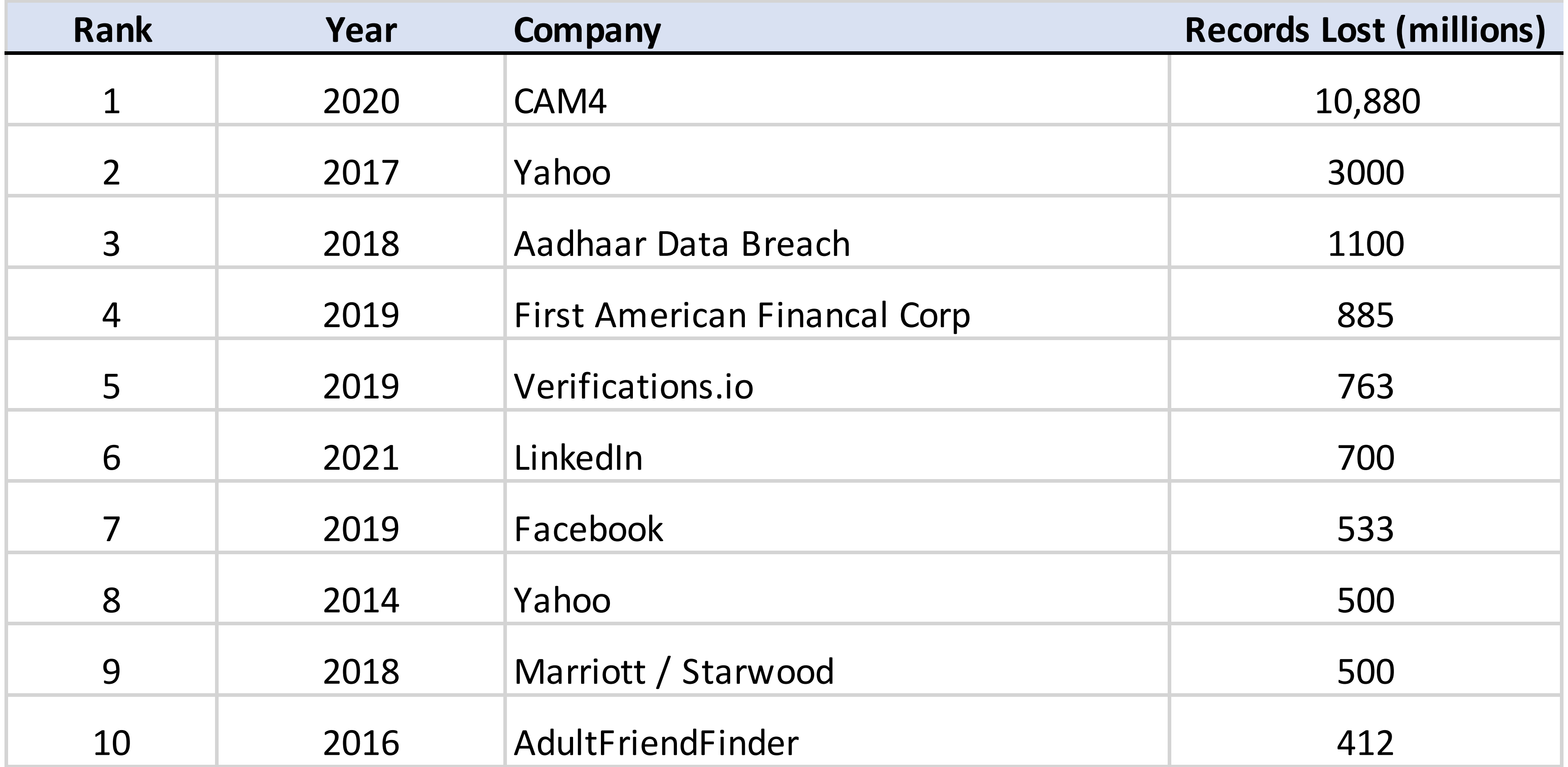
What Every Startup Needs To Know About Privacy and Cybersecurity

CONNECTS Seminar at Carnegie Mellon: OCTOBER 25, 2022
John Funge, DataTribe



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

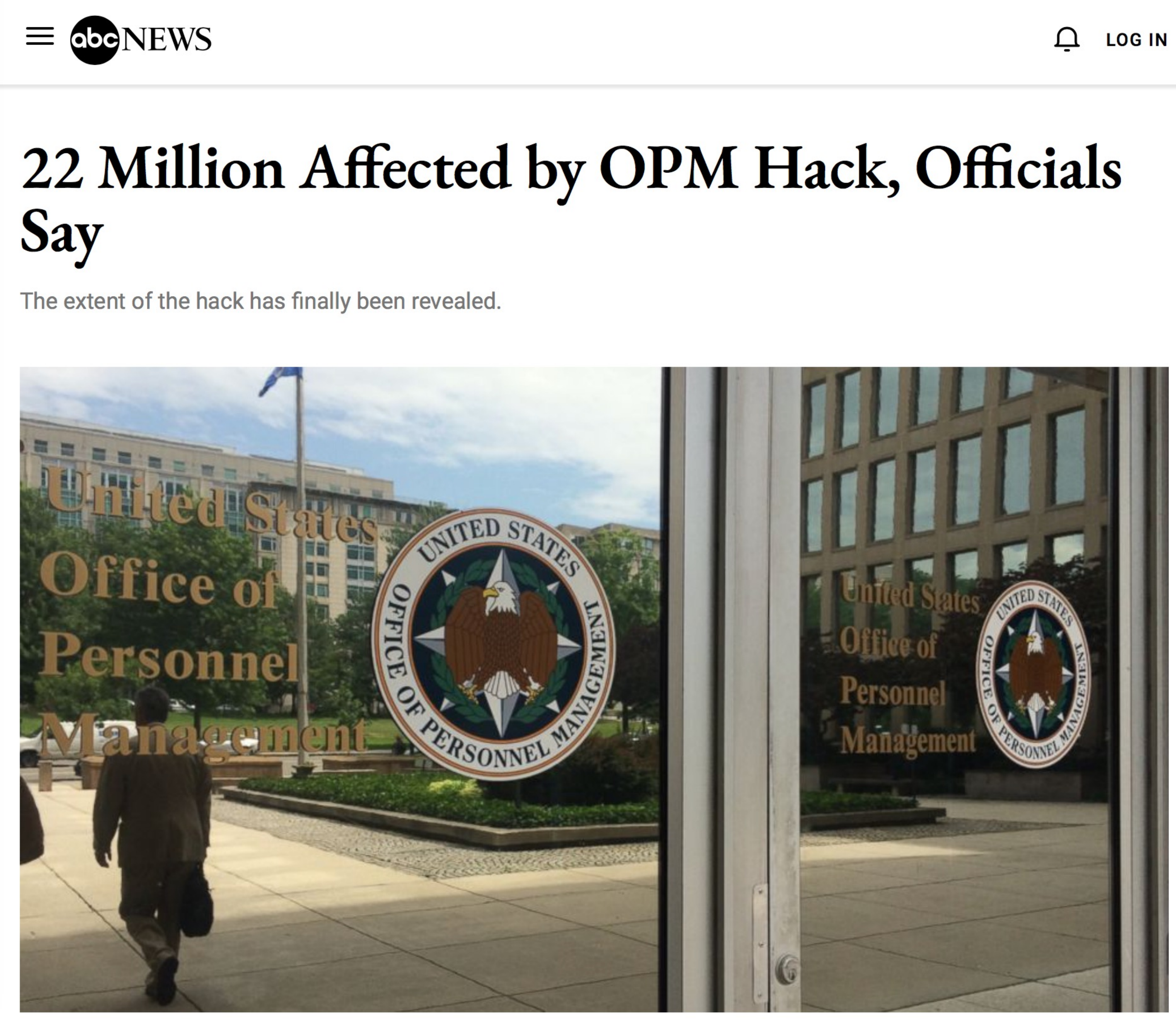
Biggest Data Breaches of the 21st Century



Rank	Year	Company	Records Lost (millions)
1	2020	CAM4	10,880
2	2017	Yahoo	3000
3	2018	Aadhaar Data Breach	1100
4	2019	First American Financal Corp	885
5	2019	Verifications.io	763
6	2021	LinkedIn	700
7	2019	Facebook	533
8	2014	Yahoo	500
9	2018	Marriott / Starwood	500
10	2016	AdultFriendFinder	412

Source: https://www.upguard.com/blog/biggest-data-breaches

~ 350 Major since 2004 in Wikipedia → 20 / year



22 Million Affected by OPM Hack, Officials Say

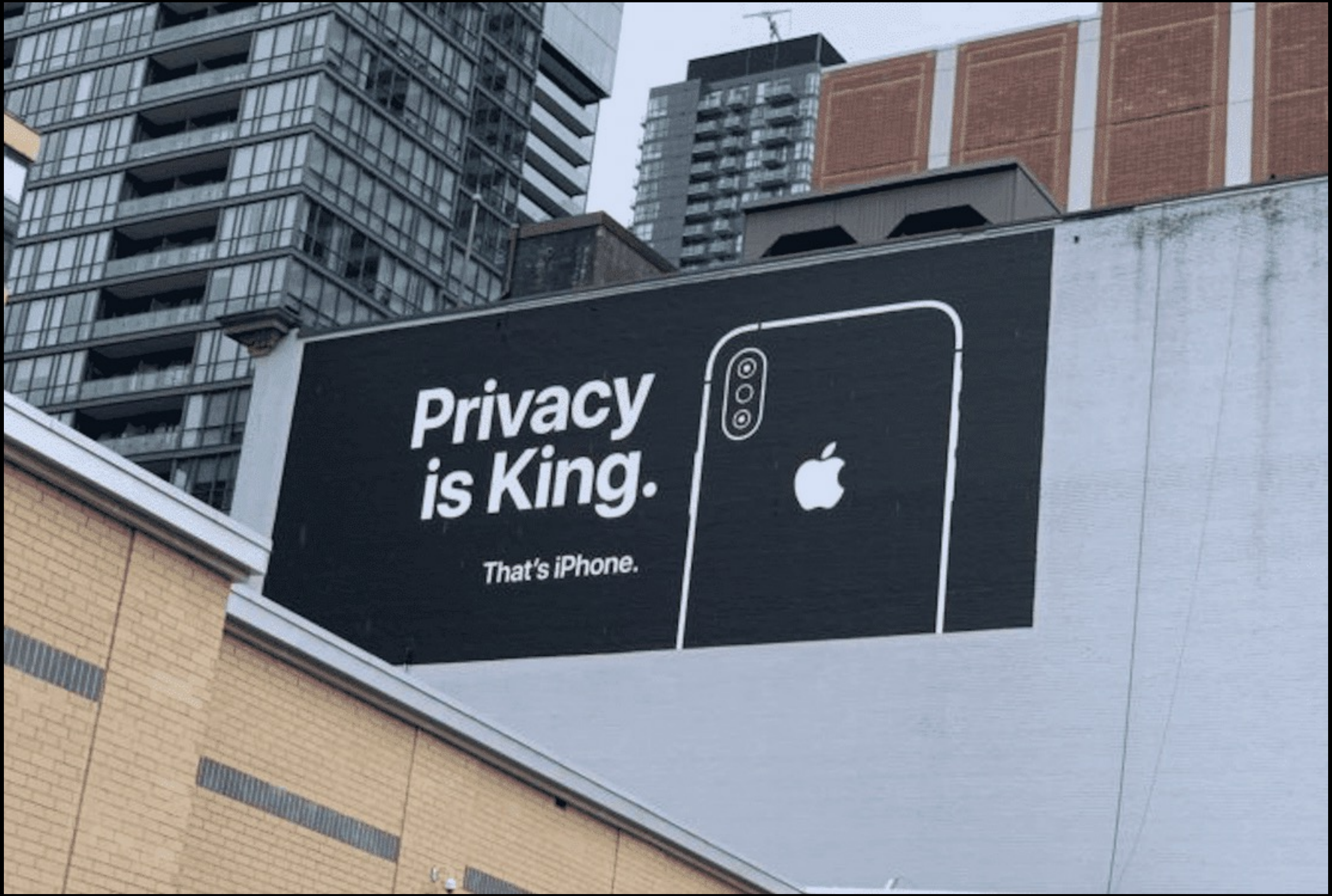
The extent of the hack has finally been revealed.

“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


Privacy is King.
That's iPhone.

“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

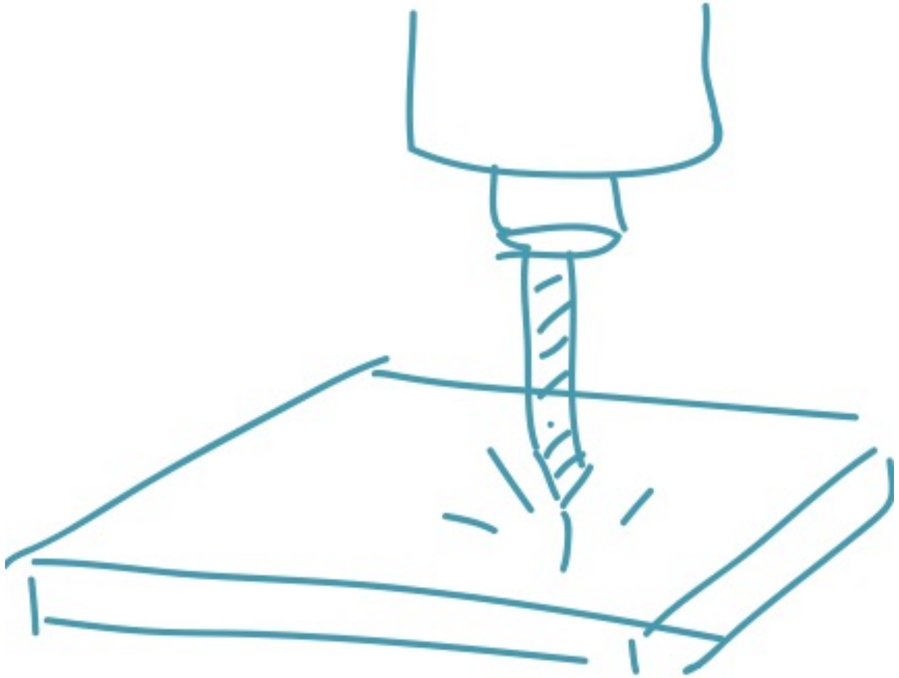
Big Picture

“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?

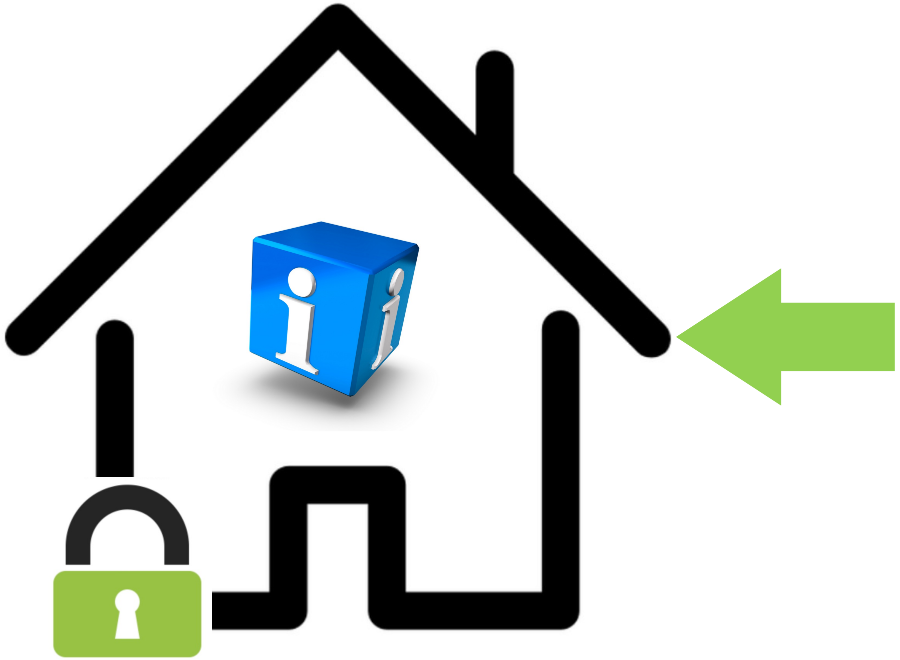
Axiom 1: Focus



Axiom 2: Stage Appropriateness

Axiom 3: Find trustworthy trail guides early

Privacy



A Sea Change in the Last 5 Years

For example…

- Privacy Management Platform
- Founded 2016
- Today
  - 2,700 Employees
  - $7B valuation as of December 2021

OneTrust
Privacy Management Software

Context

- Ever Increasing Digitalization of Life
- Cloud Computing → Democratizing Big Data
- GDPR & CCPA … and numerous others…
- 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)

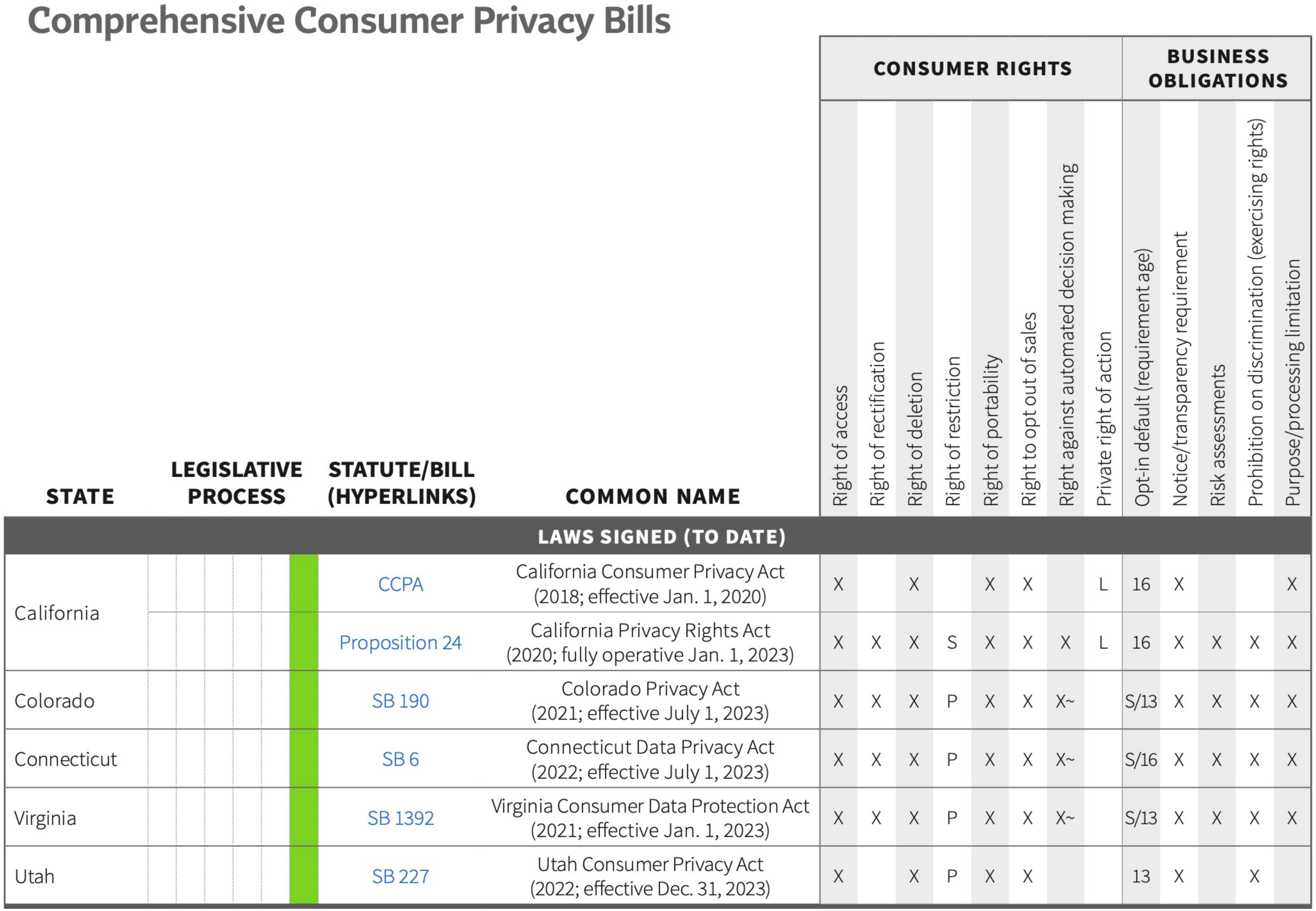
Making Sense of It All

- 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

US State Privacy Legislation Tracker 2022

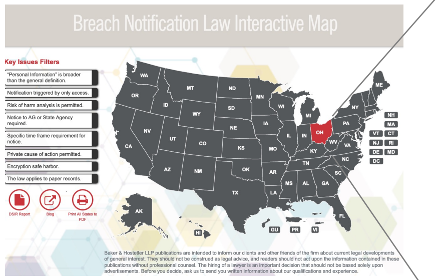


Comprehensive Consumer Privacy Bills

STATE	LEGISLATIVE PROCESS	STATUTE/BILL (HYPERLINKS)	COMMON NAME	CONSUMER RIGHTS: Right of access	Right of rectification	Right of deletion	Right of restriction	Right of portability	Right to opt out of sales	Right against automated decision making	Private right of action	BUSINESS OBLIGATIONS: Opt-in default (requirement age)	Notice/transparency requirement	Risk assessments	Prohibition on discrimination (exercising rights)	Purpose/processing limitation
LAWS SIGNED (TO DATE)																
California	🟩	CCPA	California Consumer Privacy Act (2018; effective Jan. 1, 2020)	X		X		X	X		L	16	X			X
	🟩	Proposition 24	California Privacy Rights Act (2020; fully operative Jan. 1, 2023)	X	X	X	S	X	X	X	L	16	X	X	X	X
Colorado	🟩	SB 190	Colorado Privacy Act (2021; effective July 1, 2023)	X	X	X	P	X	X	X~		S/13	X	X	X	X
Connecticut	🟩	SB 6	Connecticut Data Privacy Act (2022; effective July 1, 2023)	X	X	X	P	X	X	X~		S/16	X	X	X	X
Virginia	🟩	SB 1392	Virginia Consumer Data Protection Act (2021; effective Jan. 1, 2023)	X	X	X	P	X	X	X~		S/13	X	X	X	X
Utah	🟩	SB 227	Utah Consumer Privacy Act (2022; effective Dec. 31, 2023)	X		X	P	X	X			13	X		X	

Source: https://iapp.org/resources/article/us-state-privacy-legislation-tracker/

“Toxic Data” & Data Breach Laws

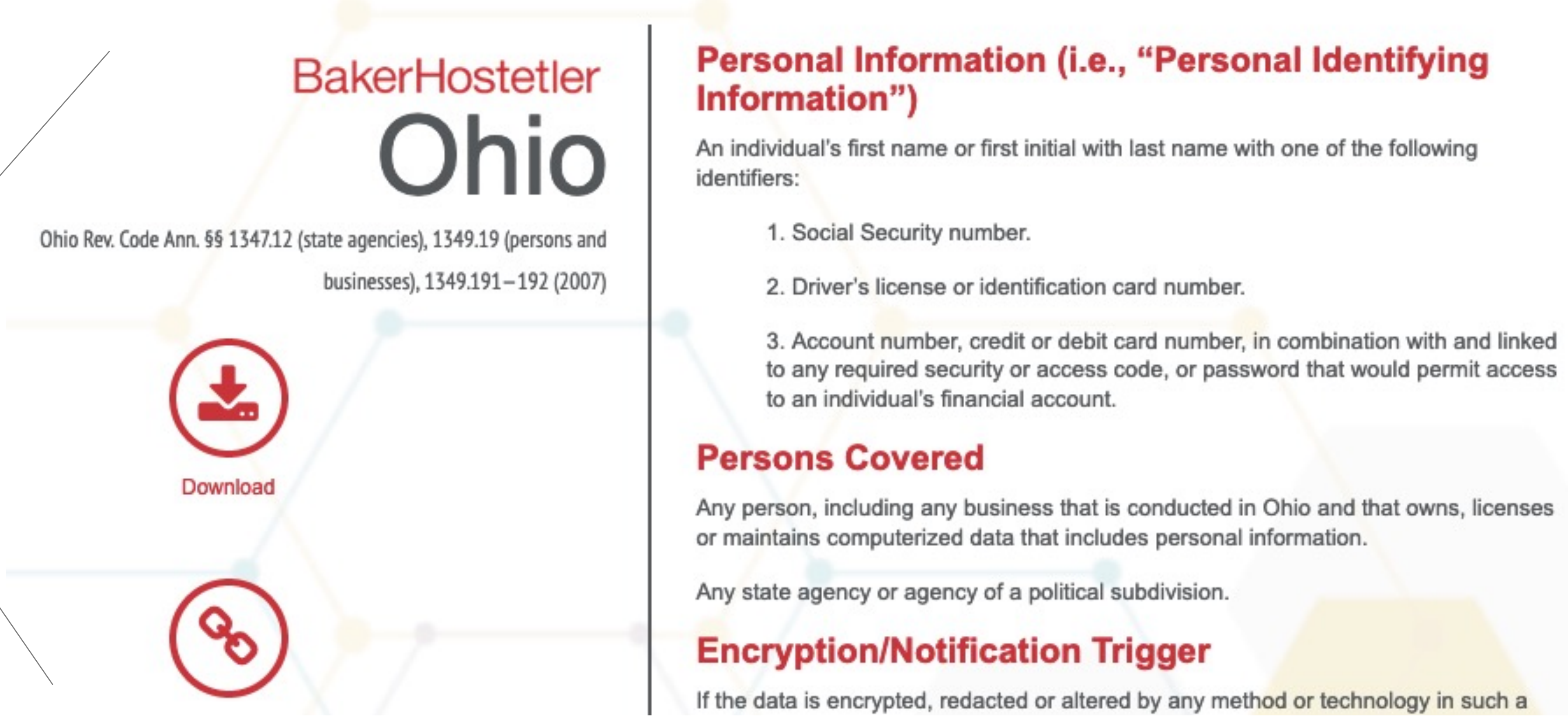


Breach Notification Law Interactive Map

Key Issues Filters

- “Personal Information” is broader than the general definition.
- Notification triggered by only access.
- Risk of harm analysis is permitted.
- Notice to AG or State Agency required.
- Specific time frame requirement for notice.
- Private cause of action permitted.
- Encryption safe harbor.
- The law applies to paper records.

Baker & Hostetler LLP publications are intended to inform our clients and other friends of the firm about current legal developments of general interest. They should not be construed as legal advice, and readers should not act upon the information contained in these publications without professional counsel. The hiring of a lawyer is an important decision that should not be based solely upon advertisements. Before you decide, ask us to send you written information about our qualifications and experience.



BakerHostetler

Ohio

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

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.

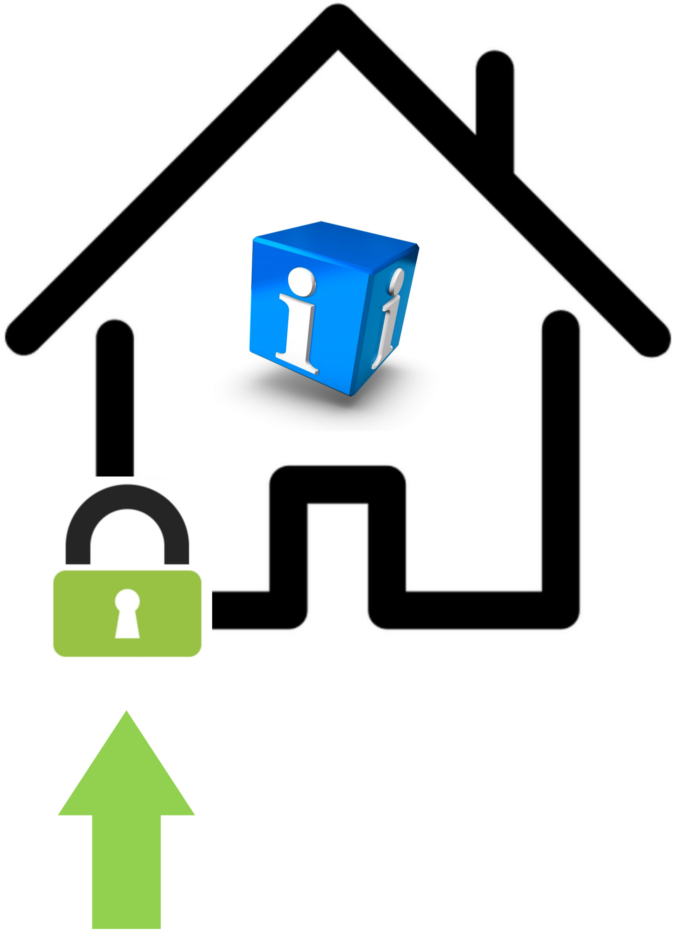
Any state agency or agency of a political subdivision.

Encryption/Notification Trigger

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

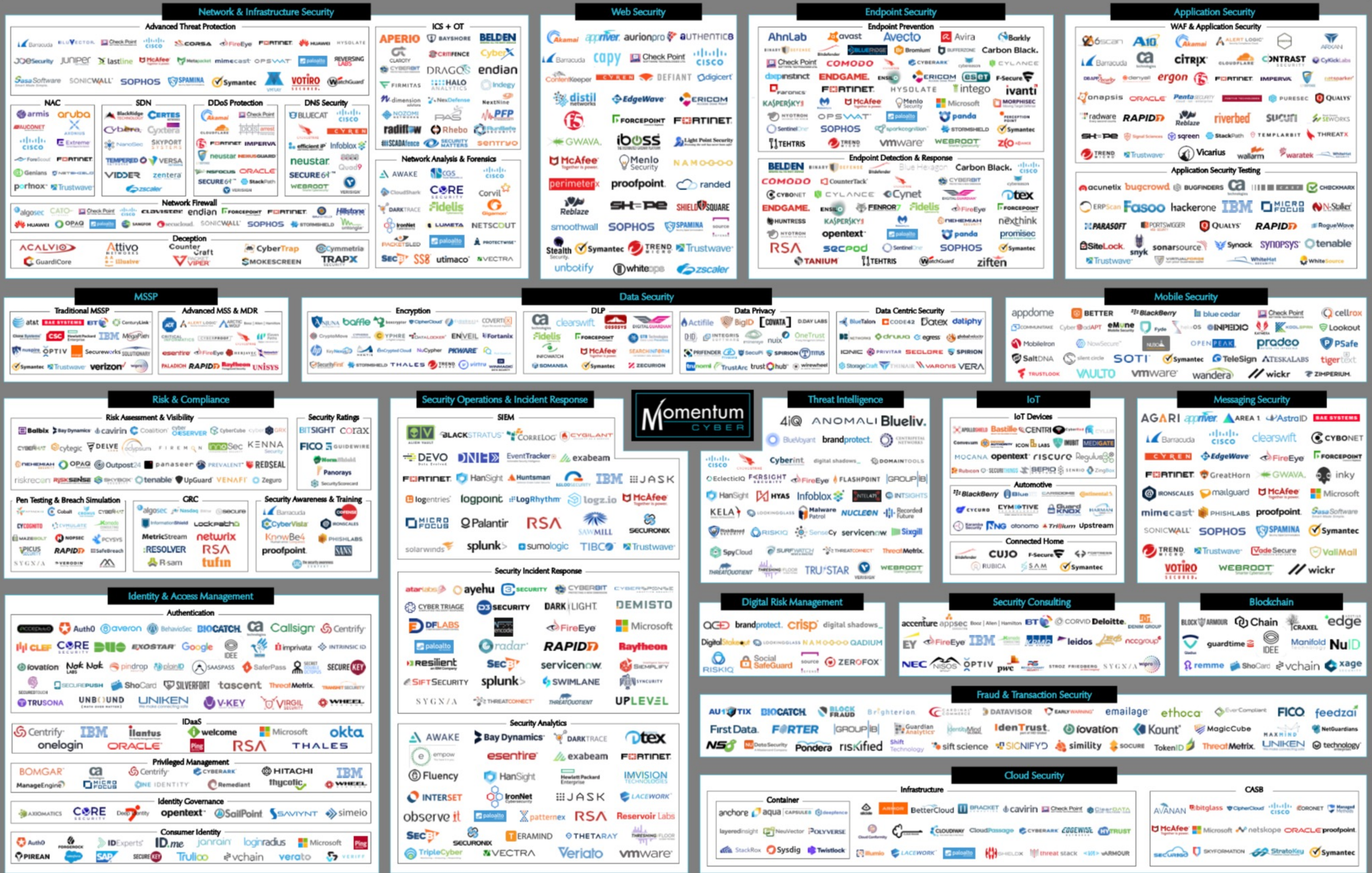
https://www.bakerlaw.com/BreachNotificationLawMap

Security



CYBERscape

v2.5



Network & Infrastructure Security

Advanced Threat Protection

Barracuda, BluVector, Check Point, Cisco, Corsa, FireEye, Fortinet, Huawei, Hysolate, Joe Security, Juniper, lastline, McAfee, Metaflows, mimecast, OPSWAT, paloalto, Reversing Labs, Sasa Software, SonicWall, Sophos, Spamina, Symantec, Vmray, Votiro, WatchGuard

NAC

armis, aruba, Auconet, Avaya, Cisco, Extreme, ForeScout, Fortinet, Genians, Portnox, Trustwave

SDN

BlackRidge, Certes, Cyberа, Cyxtera, NanoSec, Skyport, Tempered, Versa, Vidder, zentera, zscaler

DDoS Protection

Akamai, Cloudflare, Check Point, Fortinet, Imperva, neustar, Nexusguard, Radware, Secure64, StackPath, Verisign

DNS Security

BlueCat, Cisco, Cyren, efficient iP, Infoblox, neustar, Quad9, Secure64, Webroot, Verisign

ICS + OT

Aperio, Bayshore, Belden, Claroty, CritiFence, CyberX, Cyberbit, Dragos, endian, Firmitas, Halo Analytics, Indegy, dimension, NexDefense, NextNine, Nozomi Networks, PAS, PFP, radiflow, Rhebo, RunSafe, SCADAfence, Security Matters, Sentryo

Network Analysis & Forensics

Awake, CGS, Cisco, CloudShark, Core Security, Corvil, DarkTrace, Fidelis, Gigamon, IronNet, Lumeta, NetScout, PacketSled, paloalto, Protectwise, SecBI, SS8, utimaco, Vectra

Network Firewall

algosec, Cato, Check Point, Cisco, Clavister, endian, Forcepoint, Fortinet, Hillstone, Huawei, OPAQ, paloalto, Sangfor, securicloud, SonicWall, Sophos, Stormshield, Untangle

Deception

Acalvio, Attivo, Counter Craft, CyberTrap, Cymmetria, GuardiCore, Illusive, Smokescreen, TrapX, Viper

Web Security

Akamai, Appriver, aurionpro, Authentic8, Barracuda, Copy, Check Point, Cisco, ContentKeeper, Cyren, Defiant, Digicert, distil networks, EdgeWave, Ericom, F5, Forcepoint, Fortinet, GWAVA, iboss, Light Point Security, McAfee, Menlo Security, Namogoo, perimeterx, proofpoint, randed, Reblaze, Shape, Shield Square, smoothwall, Sophos, Spamina, Source Defense, Stealth Security, Symantec, Trend Micro, Trustwave, unbotify, whiteops, zscaler

Endpoint Security

Endpoint Prevention

AhnLab, avast, Avecto, Avira, Barkly, Binary Defense, Bitdefender, BlueRidge, Bromium, Bufferzone, Carbon Black, Check Point, Comodo, CyberArk, Cylance, deepinstinct, Endgame, Ensilo, Ericom, ESET, F-Secure, Faronics, Fortinet, Hysolate, intego, ivanti, Kaspersky, Malwarebytes, McAfee, Menlo Security, Microsoft, Morphisec, Nyotron, OPSWAT, paloalto, panda, Perception Point, SentinelOne, Sophos, sparkcognition, Stormshield, Symantec, Tehtris, Trend Micro, vmware, Webroot, Zilog

Endpoint Detection & Response

Belden, Binary Defense, Bitdefender, Blue Hexagon, Carbon Black, Cisco, Comodo, CounterTack, Cybereason, Cybonet, Cylance, Cynet, Cyberbit, Deep Instinct, Dtex, Endgame, Ensilo, Fenror7, Fidelis, FireEye, Forcepoint, Huntress, Kaspersky, Malwarebytes, Nehemiah, nexthink, Nyotron, opentext, paloalto, panda, promisec, RSA, secpod, SentinelOne, Sophos, Symantec, Tanium, Tehtris, WatchGuard, ziften

Application Security

WAF & Application Security

6Scan, A10, Akamai, Alert Logic, Arxan, Barracuda, CA Technologies, citrix, Cloudflare, Contrast, CyKickLabs, Dearbytes, denyall, ergon, F5, Fortinet, Imperva, Jscrambler, nsfocus, onapsis, Oracle, Pentasecurity, Prevoty, Puresec, Qualys, radware, Rapid7, Reblaze, riverbed, Sucuri, Seworks, Shape, Signal Sciences, sqreen, StackPath, Templarbit, ThreatX, Trend Micro, Trustwave, Vicarius, wallarm, waratek, WhiteHat

Application Security Testing

acunetix, bugcrowd, Bugfinders, CA, Checkmarx, ERPScan, Fasoo, hackerone, IBM, Micro Focus, N-Stalker, Parasoft, Portswigger, Qualys, Rapid7, RogueWave, SiteLock, snyk, sonarsource, Synack, synopsys, tenable, Trustwave, Virtual Forge, WhiteHat, WhiteSource

MSSP

Traditional MSSP

at&t, BAE Systems, BT, CenturyLink, Cisco, CSC, Dell, IBM, MegaPath, Nuspire, Optiv, Secureworks, Solutionary, Symantec, Trustwave, verizon, Wipro

Advanced MSS & MDR

ACM, Alert Logic, Arctic Wolf, Booz Allen Hamilton, Critical Informatics, Cyberproof, Delta Risk, eSentire, FireEye, Herjavec Group, Paladion, Rapid7, Raytheon, Unisys

Data Security

Encryption

Anuna, baffle, CipherCloud, Covata, CryptoMove, Cyphre, Datalocker, Enveil, Fortanix, Keynexus, nCipher, PKWARE, SecurityFirst, Stormshield, Thales, Trend Micro, Virtru, Winmagic

DLP

CA, clearswift, Code42, Digital Guardian, Fidelis, Forcepoint, Infowatch, McAfee, GTB Technologies, Searchinform, Somansa, Symantec, Zecurion

Data Privacy

Actifile, BigID, Covata, D.Day Labs, DID, Integris, nuix, OneTrust, Prifender, SecuPi, Spirion, Titus, TrustArc, trust hub, Wirewheel

Data Centric Security

BlueTalon, Code42, Datex, dataphy, druva, egress, globalscape, Ionic, Privitar, Seclore, Spirion, StorageCraft, Thinair, Varonis, Vera

Mobile Security

appdome, Better, BlackBerry, blue cedar, Check Point, cellrox, Communitake, CyberAdapt, eMune, fyde, iOS, iNPEDIO, Kaymera, Koolspan, Lookout, MobileIron, NowSecure, Nubo, OpenPeak, pradeo, PSafe, SaltDNA, silent circle, SOTI, Symantec, TeleSign, Teskalabs, tiger text, Trustlook, Vaulto, vmware, wandera, wickr, Zimperium

Risk & Compliance

Risk Assessment & Visibility

Balbix, Bay Dynamics, Cavirin, Coalition, Cyber Observer, CyberCube, Cyberint, GRC, Cyberstrat, cytegic, Delve, Edyssium, Firemon, InnoSec, Kenna, Nehemiah, OPAQ, Outpost24, Panaseer, Prevalent, RedSeal, riskrecon, RiskSense, SkyBox, tenable, UpGuard, Venafi, Zeguro

Security Ratings

BitSight, corax, FICO, Guidewire, NormShield, Panorays, SecurityScorecard

Pen Testing & Breach Simulation

Cobalt, Cronus, CyberArk, CyCognito, Cymulate, Kerodo, Mazebolt, Nopsec, Pcysys, Picus, Rapid7, SafeBreach, Sygnia, Verodin, XM Cyber

GRC

algosec, Nasdaq, Ignyte, secure, InformationShield, Lockpath, MetricStream, netwrix, Resolver, RSA, R-sam, tufin

Security Awareness & Training

Barracuda, CyberVista, Cofense, KnowBe4, Ironscales, PhishLabs, proofpoint, SANS, The Security Awareness Company

Security Operations & Incident Response

SIEM

Alien Vault, Blackstratus, Correlog, Cygilant, Devo, DNIF, EventTracker, exabeam, Fortinet, HanSight, Huntsman, IBM, JASK, logentries, logpoint, LogRhythm, logz.io, McAfee, Micro Focus, Palantir, RSA, SawMill, Securonix, solarwinds, splunk, sumologic, TIBCO, Trustwave

Security Incident Response

atarlabs, ayehu, D3 Security, Cyberbit, Cybersponse, Cyber Triage, D3 Security, Dark Light, Demisto, DFLabs, Endace, FireEye, Microsoft, paloalto, radar, Rapid7, Raytheon, Resilient, SecBI, servicenow, Siemplify, SiftSecurity, splunk, Swimlane, Syncurity, Sygnia, ThreatConnect, ThreatQuotient, Uplevel

Security Analytics

Awake, Bay Dynamics, DarkTrace, Dtex, empow, esentire, exabeam, Fortinet, Fluency, HanSight, Hewlett Packard Enterprise, Imvision Technologies, Interset, IronNet, JASK, Lacework, observe it, paloalto, patternex, RSA, Reservoir Labs, SecBI, Securonix, Teramind, Thetaray, Threat Stack, TripleCyber, Vectra, Veriato, vmware

Momentum Cyber

Threat Intelligence

4iQ, Anomali, Blueliv, brandprotect, BlueVoyant, Centripetal Networks, Cisco, Cyberint, Cyren, digital shadows, DomainTools, EclecticIQ, Farsight Security, FireEye, Flashpoint, Group-IB, HanSight, HYAS, Infoblox, IntSights, Intel 471, KELA, LookingGlass, Malware Patrol, Nucleon, Recorded Future, RiskIQ, SenseCy, servicenow, Sixgill, SpyCloud, Surfwatch, ThreatConnect, ThreatMetrix, ThreatQuotient, Threshing Floor, TruStar, Verisign, Webroot

IoT

IoT Devices

Apollo Shield, Bastille, Centri, Cybertrust, CyLus, Convexum, Cyberbit, Icon Labs, Mobilicom, Medigate, Mocana, opentext, riscure, Regulus, Rubicon, Securithings, Sepio, Senrio, Zingbox

Automotive

BlackBerry, Blue, Carsome, Cyclus, Cymotive, GuardKnox, Harman, Karamba Security, NNG, otonomo, Trillium, Upstream

Connected Home

Bitdefender, CUJO, F-Secure, Fortinet, Rubica, SAM, Symantec

Messaging Security

AGARI, appriver, Area 1, AstraID, BAE Systems, Barracuda, Cisco, clearswift, Cybonet, Cyren, EdgeWave, FireEye, Forcepoint, Fortinet, GreatHorn, GWAVA, inky, Ironscales, mailguard, McAfee, Microsoft, mimecast, PhishLabs, proofpoint, Sasa Software, SonicWall, Sophos, Spamina, Symantec, Trend Micro, Trustwave, Vade Secure, VailMail, Votiro, Webroot, wickr

Identity & Access Management

Authentication

Acceptto, Auth0, averon, BehavioSec, BioCatch, CA Technologies, Callsign, Centrify, Clef, Core Security, Duo, Exostar, Google, IDEE, imprivata, Intrinsic ID, iovation, Nok Nok, pindrop, plainID, SaasPass, SaferPass, Secret Double Octopus, SecureKey, Securetouch, SecurePush, ShoCard, Silverfort, tascent, ThreatMetrix, Transmit Security, Trusona, Unbound, Uniken, V-Key, Virgil, Wheel

IDaaS

Centrify, IBM, Ilantus, welcome, Microsoft, okta, onelogin, Oracle, Ping, RSA, Thales

Privileged Management

Bomgar, CA, Centrify, CyberArk, Hitachi, IBM, ManageEngine, Micro Focus, One Identity, Remediant, thycotic, Wheel

Identity Governance

Axiomatics, Core Security, Deep Identity, opentext, SailPoint, Saviynt, simeio

Consumer Identity

Auth0, ForgeRock, IDExperts, ID.me, janrain, loginradius, Microsoft, Ping, Pirean, Salesforce, SAP, SecureKey, Trulioo, vchain, verato, Veriff

Digital Risk Management

AGARI, brandprotect, crisp, digital shadows, Digital Stakeout, LookingGlass, Namogoo, Qadium, RiskIQ, Social SafeGuard, Source Defense, ZeroFox

Security Consulting

accenture, appsec, Booz Allen Hamilton, BT, Corvid, Deloitte, Denim Group, EY, FireEye, IBM, Kroll, leidos, nccgroup, NEC, Nisos, Optiv, pwc, Raytheon, Stroz Friedberg, Sygnia, wipro

Blockchain

Block Armour, Chain, Craxel, edge, guardtime, IDEE, Manifold, NuID, remme, ShoCard, vchain, xage

Fraud & Transaction Security

AU10TIX, BioCatch, Block Fraud, Brighterion, Cardinal Commerce, Datavisor, Early Warning, emailage, ethoca, EverCompliant, FICO, feedzai, First Data, Forter, Group-IB, Guardian Analytics, IdentityMind, IdenTrust, iovation, Kount, MagicCube, MaxMind, NetGuardians, NS8, OneSpan, Pondera, riskified, Shift Technology, sift science, SIGNIFYD, simility, Socure, TokenID, ThreatMetrix, Uniken, Vesta

Cloud Security

Infrastructure

Armor, BetterCloud, Bracket, cavirin, Check Point, CloudCheckr, Cloud Conformity, Cloudvisory, Cloudpassage, CyberArk, Edgewise, Lumio, Lacework, paloalto, Shieldx, threat stack, Armour

Container

anchore, aqua, Capsule8, deepfence, layeredinsight, NeuVector, Polyverse, StackRox, Sysdig, Twistlock

CASB

Avanan, bitglass, CipherCloud, Cisco, Coronet, Managed Methods, McAfee, Microsoft, netskope, Oracle, proofpoint, Securlog, Skyformation, StratoKey, Symantec

A Simple Way of Breaking It Down

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

General Guidelines

- Focus on doing the basics well

- Invest where there is risk

Top 5 Checklist

From Harvard Belfer Center Cybersecurity Campaign Playbook

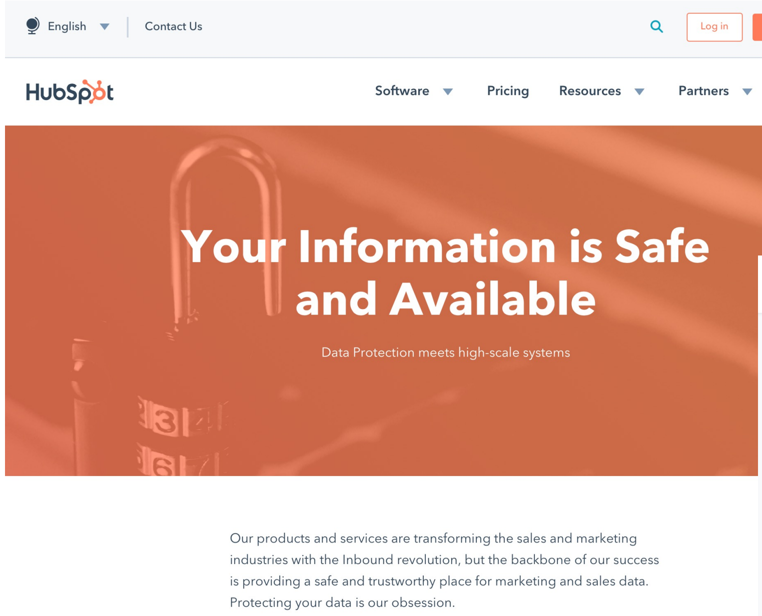
1. Establish a culture of security awareness
2. Use the cloud
3. Use two-factor authentication
4. Encrypted messaging for sensitive comm.
5. Plan and prepare

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

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

Other Things to Keep in Mind

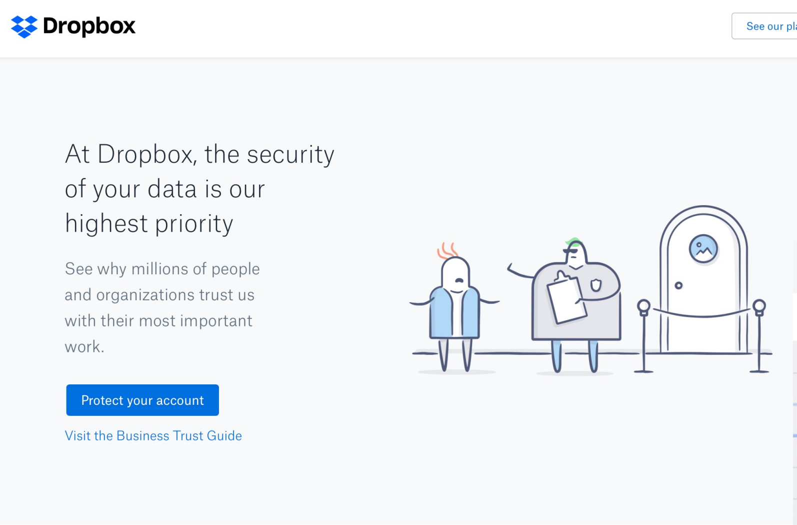
Third Party Risk



Your Information is Safe and Available

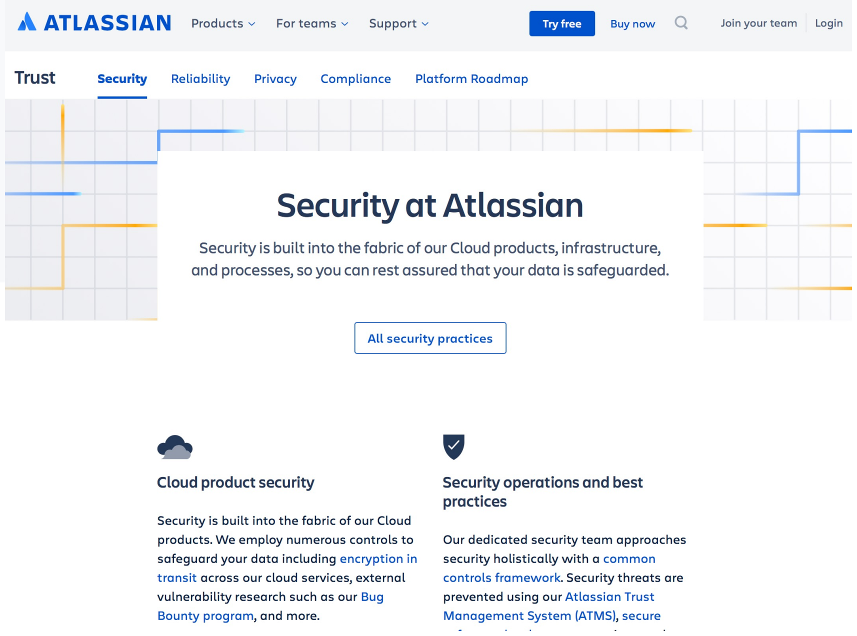
Data Protection meets high-scale systems

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.



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.



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.

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

DevSecOps

OWASP

Top 10

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

snyk

sonatype

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

Audio

Email

“Complexity is the worst enemy of security…”

Schneier, Bruce. *Data and Goliath*

Thank You

John Funge
DataTribe
john.funge@datatribe.com