RSAConference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **SAT-T01**

Where Humane Technology & Secure Technology Meet

Corey Jackson

President & Chief Security Strategist
SACRO LLC
@LLCSACRO

Lisa LeVasseur

Executive Director
Internet Safety Labs (was Me2B Alliance)
@Me2BAlliance

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

RSAConference2022

A Word About Words

“Privacy vs. Security” framing is a false dichotomy.

And “privacy & security” is a category error.

The subject of *privacy* is:

People

Photo by Thought Catalog on Unsplash

The subject of *security* is:

IT Systems

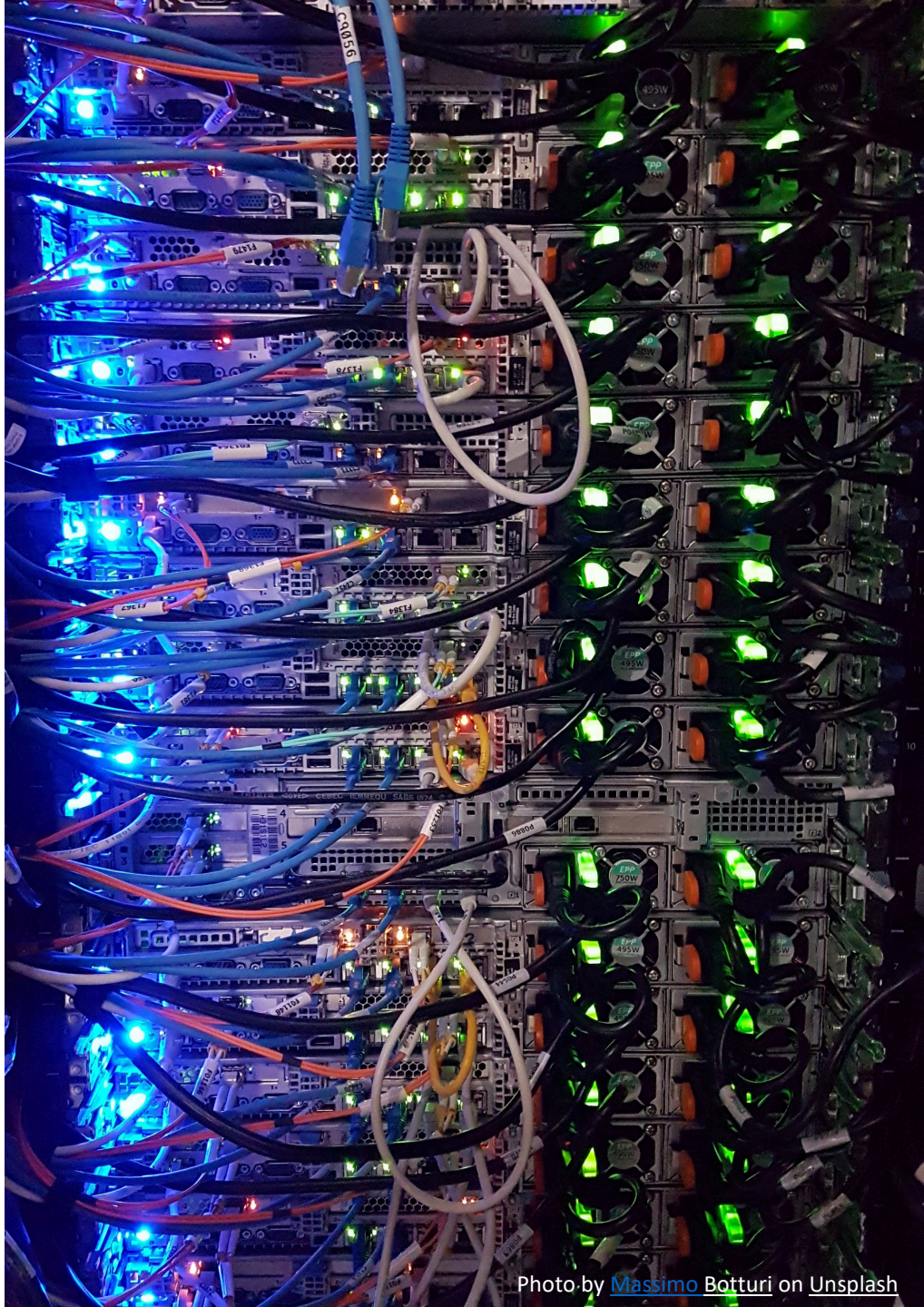

Photo by Massimo Botturi on Unsplash

What is Humane Technology?

Humane technology **is**

safe and respectful

technology.

For people.

Safety includes respecting personal boundaries.

Such as privacy.

It’s not about *privacy* vs. *security*.

It's about *safety* AND *security*.

The digital world must be *safe* AND *secure.*

RSAConference2022

Premise of This Talk

PREMISE:

Systemic challenges to producing safe technology are the SAME systemic challenges to producing secure technology.

* sometimes

RSAConference2022

Common Challenges

Common Systemic Challenges

1. Development related
2. User Experience related
3. Business related
4. Professional Development related
5. Industry Standards & Regulatory related

1. Development Related Challenges

CHALLENGE	SECURE TECHNOLOGY	SAFE TECHNOLOGY
Software Complexity	Challenges ability to address all threat surfaces. Lack of ownership/responsibility.	Challenges ability to ensure safe & respectful behavior.
Increasing Reliance on Third Party Software Components	Vulnerable 3rd party libraries, supply chain attacks, and/or data breaches	Immature vetting and evaluation criteria.
Must Be Built-in From the Start / Can't Retrofit	Inadequate training, Apps, and patching maturity leading to security gaps. Secure by design.	Interwoven automated decision-making; unknown data supply flow. Safe by design.
Identity Management	Archaic, attractive attack vector. Password nuances <Proliferation of credentials>	Lack of anonymity; invisible over-identification of people.

1. Development Related Recommendations

CHALLENGE	RECOMMENDATIONS
Software Complexity	Systematic complexity measurement. Rigorous AppSec practice (Dev – to – Prod – to – ConMon)
Increasing Reliance on Third Party Software Components	Regular Data Supply Auditing. SW Vendor management rigor. Interoperable permission management control frameworks. Deploy effective 3rd Party Risk Mgmt. Program (TPRM)
Must Be Built-in From the Start/Can't Retrofit	Privacy by Design, Safe by Design, Secure by Design. DevSecOps, Security hygiene/shared responsibility.
Identity Management	Identification Minimization. DIDs and VCs. Position Identity and Access Mgmt services as the "new perimeter".

IDENTIFICATION MINIMIZATION

2. User Experience Challenges

CHALLENGE	SECURE TECHNOLOGY	SAFE TECHNOLOGY
Introduces friction to the user experience	Security measures perceived to introduce friction into the UX.	Safe & respectful technology can introduce friction into the UX.
Consent / Permission / Preference Management	Should be invisible to people. Don't put onus on users to keep systems or data they entrusted to you to keep safe.	Visible, uncoerced, informed permission is crucial to respectful tech. Current implementations nascent & ill-conceived. Particularly challenging in VR.

The Cookie Consent Fiasco

Privacy and cookies policy

Last updated: 18 February 2021

At Tesco, we're working hard to serve shoppers a little better every day. Looking after the personal data you share with us is a hugely important part of this. We want you to be confident that your data is safe and secure with us, and that you understand how we use it to offer you a better and more personalised shopping experience.

- What this policy covers
- Personal data we collect when we interact with you
- COVID-19 Update
- Why we collect the data we collect and why we are allowed to use that personal data
- Our Legitimate Interests in using your personal data
- Sharing personal data with Retail Partners and Service Providers
- Sharing personal data with other organisations
- How we protect your personal data
- How long we use personal data for
- Cookies and similar technologies
- Third parties operating through our Websites and Mobile App
- Your choices when it comes to cookies
- Subject access rights

Print

We reserve the right to change the policy at any time, so please check back regularly to keep informed of updates to this Policy.

Goes on…

Third parties operating through our Websites and Mobile App

Our key partners are listed below with information about the services they provide to us. This list is not exhaustive but it does include those partners with whom we have an established relationship and whose cookie technologies are most frequently deployed through our Services.

Measurement & Personalisation

To analyse how our services are used, including to test different content versions. This data may also be used to enable us to personalise our services and the marketing of our services.

- Adobe
- Optimizely
- Google
- Integral Ad Science
- Leanplum

Product recommendations

To enrich your shopping experience by delivering personalised recommendations to you on some of our websites (e.g. on Tesco Direct and F&F Clothing).

- Rich Relevance

Online marketing

To personalise Tesco adverts shown to you via Tesco and on other websites based on your interactions with Tesco. For example, by using data about your transactions with Tesco, what you have in your basket and the pages and products you look at. We may also use your Clubcard data to better personalise our marketing.

- Bing
- Google

...and on

Social media

To market to you via social media platforms and to enable social sharing and engagement on our websites. These companies may use your data for their own purposes, including to profile and target you with other advertising.

- Facebook
- Twitter
- RadiumOne (po.st)

Commenting

To power commenting on our websites (e.g. Tesco Real Food)

- Disqus

Delivering ads for our Retail Partners

To enable us to personalise and deliver online advertising on behalf of our Retail Partners.

- Google

Security of our websites and apps

To enable us to personalise and deliver online advertising on behalf of our Retail Partners.

- Akamai

2. User Experience Recommendations

CHALLENGE	RECOMMENDATIONS
Introduces Friction to the user experience	Simplify/standardize User-based security actions and responsibilities. Friction isn't all bad.
Consent/ Permission/ Preference Management	Be transparent to Users (plain and brief), informing them what they are consenting to when creating access ID/data birth rights. Ultimately support machine readable user-proferred permission policies (IEEE P7012).

FRICTION CAN BE GOOD.

IT CAN
REDUCE RISK.

3. Business Related Challenges

CHALLENGE	SECURE TECHNOLOGY	SAFE TECHNOLOGY
Surveillance for Fun & Profit	A risk to security. Impact to C.I.A Triad ***Confidentiality***	A risk to privacy and personal agency.
Supply Chain Management	More mature; security requirements and 3rd party/open-source SBOM validation. Licensure vs. Vulnerable	Non-existent/nascent criteria in SLAs. Too many "developers", org doesn't know/measure data supply flow.
Pressures for TTM and Innovation	Challenges ability to take necessary time to ensure secure technology.	Challenges ability to ensure safe & respectful behavior.
Fragmented Ownership	All C-level execs need to understand **secure** technology duties.	All C-level execs need to understand **safe** technology duties.

3. Business Related Recommendations

CHALLENGE	RECOMMENDATIONS
Surveillance for Fun & Profit	AdTech needs overhaul. Changes afoot. Early days on regulation re: surveillance for community safety.
Supply Chain Management	Add safety requirements to SW agreements; make sure you have information use & sharing limitations/data ownership. Implement Software Bill of Materials.
Pressures for TTM and Innovation	Prioritize **safe** and **secure** over innovation or jumping on tech bandwagons, and time-to-market. Build cost for safe and secure into $ and time schedules.
Fragmented Ownership	It should be everyone's job to ensure safe and secure technology.

TECH SAFETY & SECURITY IS EVERONE'S JOB.

4. Professional Development Challenges

CHALLENGE	SECURE TECHNOLOGY	SAFE TECHNOLOGY
Engineering Curriculum	Applied technical cybersecurity education and training validation prior to role assignment/acceptance.	Multi-disciplines including ethics, sociology, etc. not in engineering curriculum
Professional Credentials & Oversight	Existent. Duplication in industry. Cyber/Info-security certification governing bodies are competing and for profit.	Non-existent. Some development standards; relatively nascent.
Continuing Advanced Education	Technology and security threats are continually advancing.	Programmatic harms are constantly evolving.

4. Professional Development Recommendations

CHALLENGE	RECOMMENDATIONS
Engineering Curriculum	Cyber/Info-security must move away from elective or minor based curriculums to 100% applied science degree offerings. Safe Tech: nonexistent, considerable change needed. Early stage efforts: All Tech is Human, and many others.
Professional Credentials & Oversight	Cyber/Info- security certifications continue to train/certify practitioners in the spirit of good cause and standards, not profits. Safe Tech: nonexistent, need to develop accreditation for safe development expertise.
Continuing Advancing Education	Provided resources (education and tools/solutions) for all users/all levels. Simplified approach. Safe Tech: nonexistent, needs to be developed.

SECURITY PROFFESSIONAL DEV NEEDS MORE APPLIED PRACTICE & EVERGREEN

SAFETY PROFFESSIONAL DEV NEEDS TO EXIST.

5. Industry Standards & Regulatory

CHALLENGE	SECURE TECHNOLOGY	SAFE TECHNOLOGY
Industry Standards	Mature and robust, however repetitive with increased documentation ISO vs. NIST vs. HITRUST vs DSS PCI vs. etc.	Burgeoning; difficult to agree on universal ethical standard. These standards should be freely available, but aren't.
Regulation	Ever growing and duplicative, independent/for profit compliance complicates prioritization.	No meaningful US national regulation. Global regulation hodge-podge and incomplete.

5. Industry Standards & Regulatory Recommendations

CHALLENGE	RECOMMENDATIONS
Industry Standards	Security standards: simplified common framework, one effort application to many/all. Safety standards: Lots of privacy and ethics work in progress in several orgs. Need more participation from NON-STEM experts—psychologists, sociologists, philosophers. Key challenge here is that safe has legal implications, so must ultimately align law and safety standards. Safety <and security> specs should be free.
Regulation	Security Regulation: Regulator led, shift from independent for-profit compliance frameworks/bodies to Common Cybersecurity Compliance Model© Safety Regulation: Currently no legal/regulatory consensus on what "safe" means for intangible harms. No agreement on "digital harms" or damages. Need US federal regulation.

SECURITY STDS & REG TOO MATURE.

SAFETY
STDS & REG
TOO IMMATURE.

NEED SAFETY STANDARDS & REGS, NOT JUST PRIVACY.

RSAConference2022

Solutions

Educate + Learn = Apply

Identify key “two-fer” areas in your product/org.

Self-audit product for safety.*

Tackle one systemic change.

* If you’re here you’re probably already doing security audits.

Apply What You Have Learned Today

- Identify
  - Recognize systemic safe & secure “two-fers” in your product or org
- Tackle one systemic change
  - Development, UX, or Business practices
    - Where you have influence over all stakeholders
  - Perform a safety audit on your product https://me2ba.org/safetechspec/
  - Audit your software supply chain management
    - Create a full Software Bill of Materials for your product
    - Develop new SLA terms that have safety requirements.
- Define, measure and implement impacts (ongoing)
  - Measure safety
  - Measure security

RSAConference2022

Thank You!