FUTURE OF PRIVACY FORUM

The Conjunction: Where Privacy, Security, and AI meet

Amie Stepanovich
FPF VP, US Policy

About FPF

FPF Global Offices:
DC
Brussels
Singapore
Tel Aviv

The Future of Privacy Forum (FPF) is a global non-profit organization based in Washington, DC that brings together academics, civil society, government officials, and industry to evaluate the societal, policy, and legal implications of data uses, identify the risks, and develop appropriate protections.

FUTURE OF PRIVACY FORUM

FPF Members & Team

200+ Companies

20+ Civil Society

45+ Academics

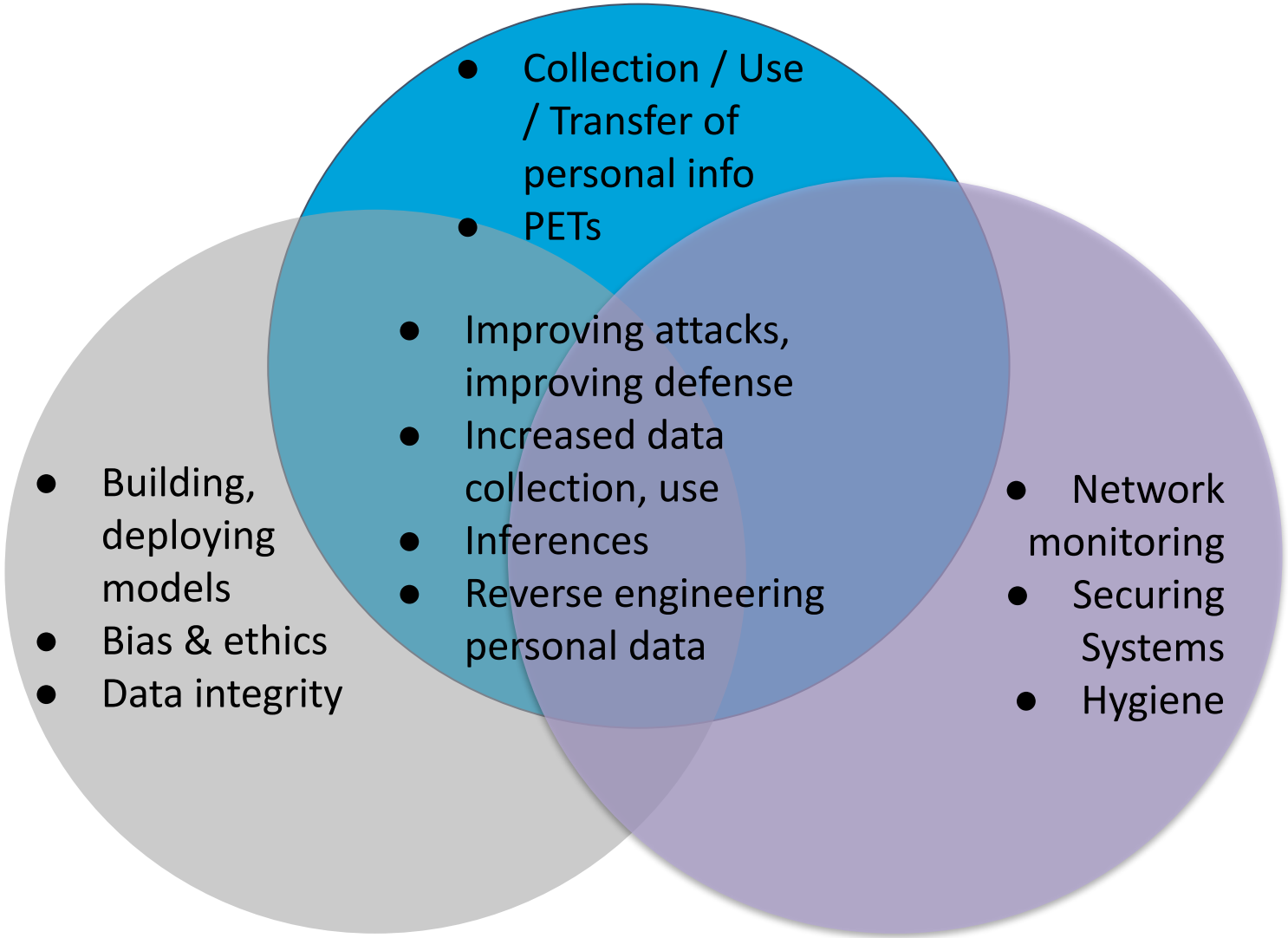
50+ Staff and Fellows

FPF Workstreams

- Legislative/Regulatory Engagement
- Ethics, Fairness, and Civil Rights
- Algorithms & AI
- Ad Tech & Platforms
- Data Sharing
- Health & Biometrics
- Youth & Education
- Data & Mobility
- Cybersecurity
- New Initiatives (e.g. finance, employment)

FUTURE OF PRIVACY FORUM

The Conjunction



Regulating in the conjunction - Overview!

- Data protection laws provide protections for personal data that extend meaningfully into AI environments
- No US federal comprehensive law for data protection, cybersecurity, and/or AI
- FTC Act - gives FTC authority over unfair and/or deceptive trade practices
  - Has been used for issues related to both privacy and security, specifically looking at AI + automated decisionmaking
    - Recent Rite Aid settlement, for instance, provides important details about Algorithimic governance programs
- Other sectoral laws
  - HIPAA, FERPA, etc.

Regulating in the conjunction: States

- Data Protection/Privacy
  - A growing number of states have passed comprehensive legislation
  - Other states have broad sectoral laws
    - e.g. WA (My Health, My Data) and Nevada; IL (BIPA)
  - Rights for individuals + organizational obligations. ALSO many have a right to opt out of automated processing, implicating AI
- Data Breach
  - Laws in all 50 states, as well as in D.C., Guam, PR, and the Virgin Islands
  - Various requirements and standards
    - In many laws it is limited to financial data and/or data related to a specific identifier (like a driver's license number)

Regulating in the conjunction: States

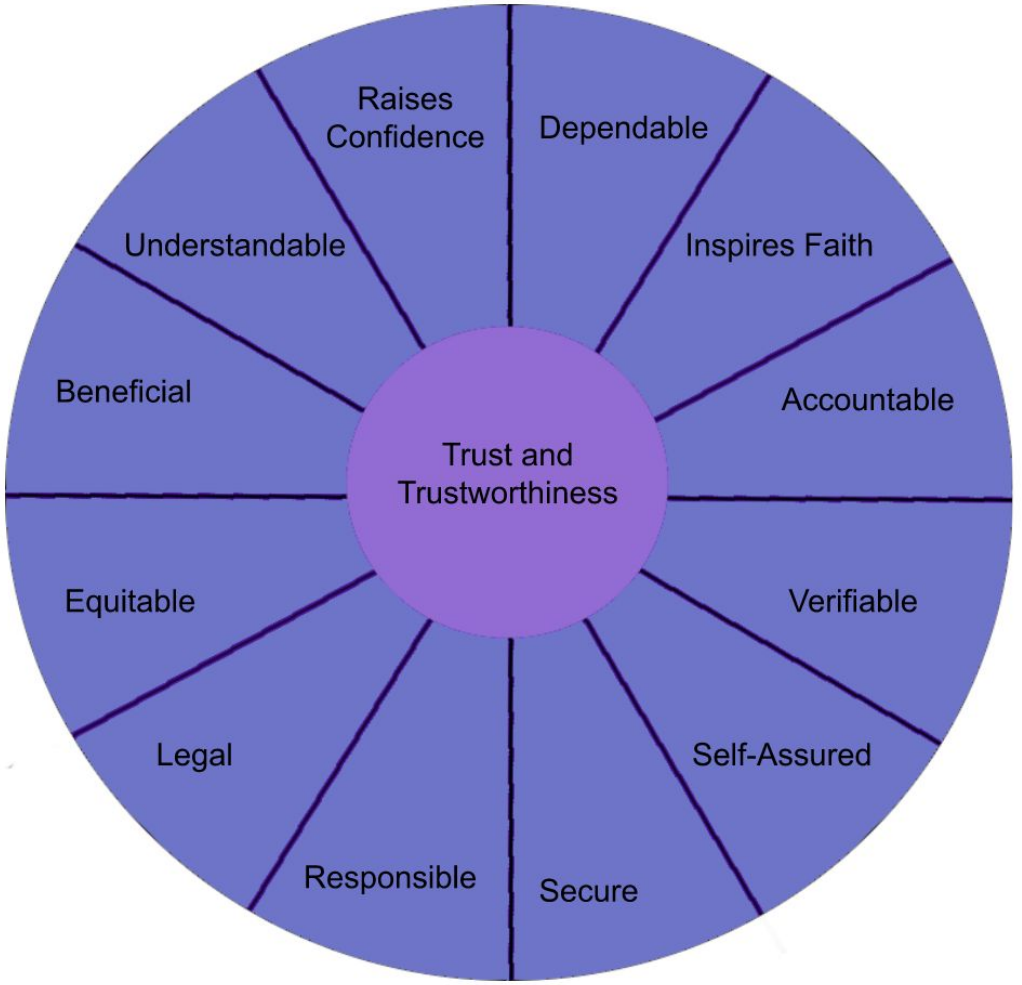
- AI
  - Comprehensive, Sectoral, or Use-Based
    - Colorado AI Act
      - High-Risk AI Systems
      - Creates obligations (developer, deployer) and rights and requires disclosures
    - California
      - 17 bills signed in 30 days, including those related to:
        - CSAM, NCII, impersonation, transparency and provenance, elections content, literacy, health care, and education
      - Vetoed a bill related to “frontier models”
    - NY City Local Law 144, IL HB 3773 (employment); GA HB 887 (healthcare)

Regulating in the conjunction: Rules

- Many states + the White House have issued Executive Orders on the topic of AI
  - Major themes include: calling for more analysis of technologies & their impact [+ policy recommendations]; policies and protections for state use of AI
- Federal
  - Many federal agencies touch on privacy, cybersecurity in specific contexts
    - Example: SEC, HHS
  - FTC has general regulatory reach - in the midst of rulemaking (MagMoss)
  - AI efforts (sample!)
    - NIST (Nat'l Institute for Standards & Technologies) Risk Mgmt Framework
    - NTIA (Nat'l Telecommunications and Information Administration) AI Accountability Policy Request for Comment
- States
  - Some state privacy laws provide space for regulations
  - CA (CPPA draft regs); CO ("human reviewed" "human involved" processing)

Challenges

- Trust
  - We have highly unrefined language around the concept of “trust”
  - People identify trust / trustworthiness as a main driver in personal choices
- Education
  - Subsets of tech literacy - privacy literacy, security literacy, and now AI literacy
  - “Book smart is not tech smart”

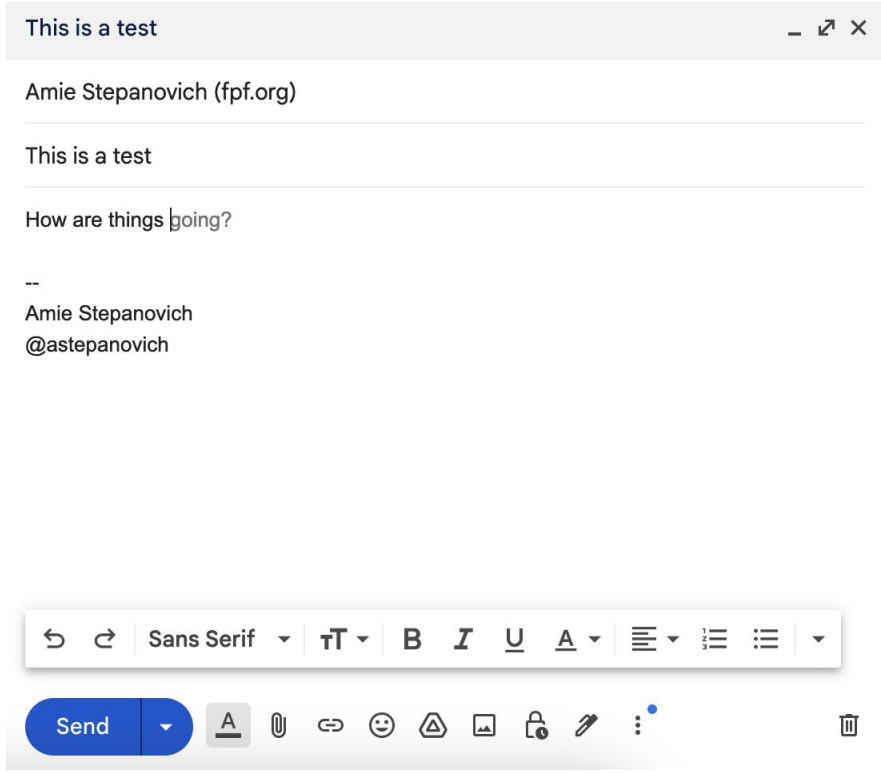


Challenges

- Bias and Discrimination
  - Reflection of society's past and present bias but with a new air of authority
  - Answer is often more data - but do people want to give their data to a system that they don't UNDERSTAND or HAVE CONFIDENCE IN?
    - FTC has started to push data disgorgement as a remedy in enforcement actions (see: Rite Aid)

Challenges

- “Averagization” and Autonomy
  - What is the most likely next thing based on the things that have come before?
  - Not necessarily a lack of creativity, but a nudge toward the middle of the bell curve
    - The curve may change based on the body of data being surveyed (is it the most likely thing for you or for anyone in your circumstances?)



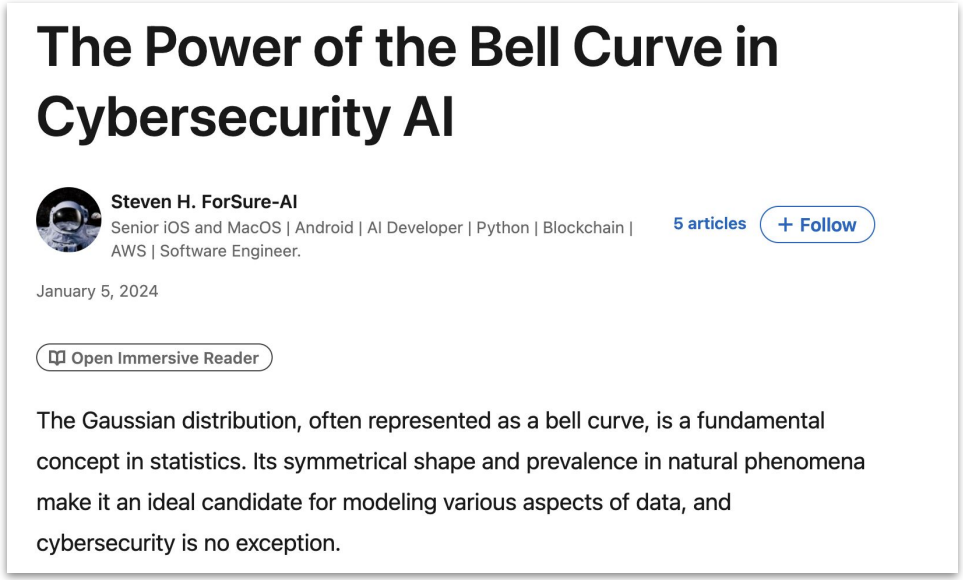
Challenges...and Opportunities

- Choosing the right use cases for AI
  - AI is EVERYWHERE - but should it be?
    - Ask - what is it good at? where is it useful? how does it add to or detract from an experience?

Planning Vacations Is More Fun Than Actually Traveling

by Gary Leff on May 15, 2021

American Express 'Amex Trendex' finds that "76% of U.S. consumers surveyed agree they instantly feel happier the moment that they book a trip." Booking travel makes people happy, but note that the survey didn't find people happier *when they actually travel*. Research has long shown that thinking about and working through the details of a trip, and then anticipating going, brings more happiness than actually going.



The Power of the Bell Curve in Cybersecurity AI

Steven H. ForSure-AI
Senior iOS and MacOS | Android | AI Developer | Python | Blockchain | AWS | Software Engineer.

5 articles + Follow

January 5, 2024

Open Immersive Reader

The Gaussian distribution, often represented as a bell curve, is a fundamental concept in statistics. Its symmetrical shape and prevalence in natural phenomena make it an ideal candidate for modeling various aspects of data, and cybersecurity is no exception.

Opportunities

- Regulating with Intention
  - To regulate or not to regulate
    - The first two decades after the commercialized internet featured a very long discussion on IF privacy should regulated
    - With AI, there is a very broad consensus that the question is not IF, but HOW regulation should occur
      - Generally, there is even consensus that a risk based model is necessary
  - This provides space to get into specifics and have nuanced conversations
  - Regulation must be robust but also workable, scalable, and consistent

Opportunities

- Big questions regulation should address
  - How to define harm and risk
    - Learn from data breach regulation and how to define harm
    - Ensure harm is considered for individuals, communities, and society
  - Need to distinguish between market participants - what a developer has access to is not the same as a deployer (and vice versa)
  - Standards and certification to ensure there is a market for any process-based governance requirements

Questions?