



RUTGERS UNIVERSITY
School of Social Work
Information Technology

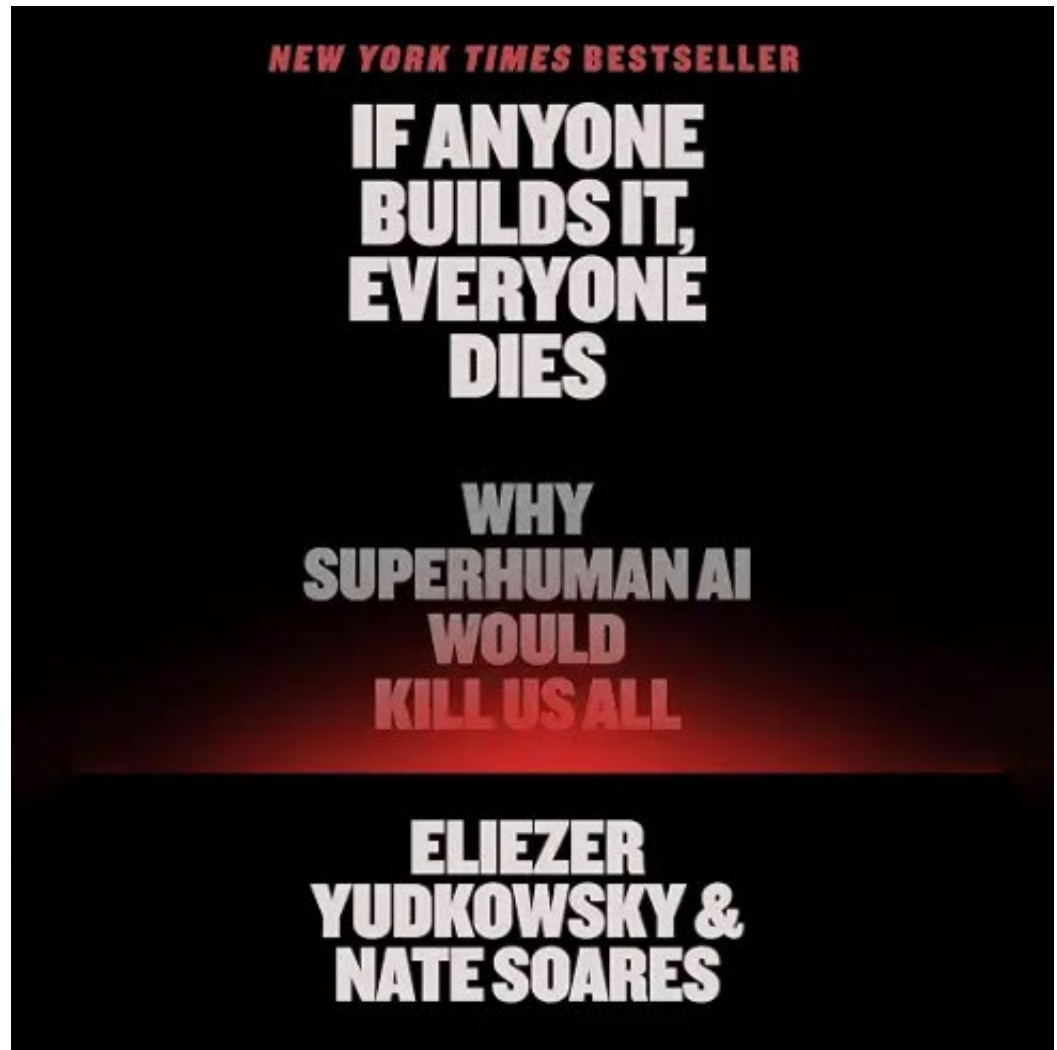
October Is Cybersecurity Month

2026 – The Year of AI Security
(Black October of Vulnerabilities)

Tibor Purger

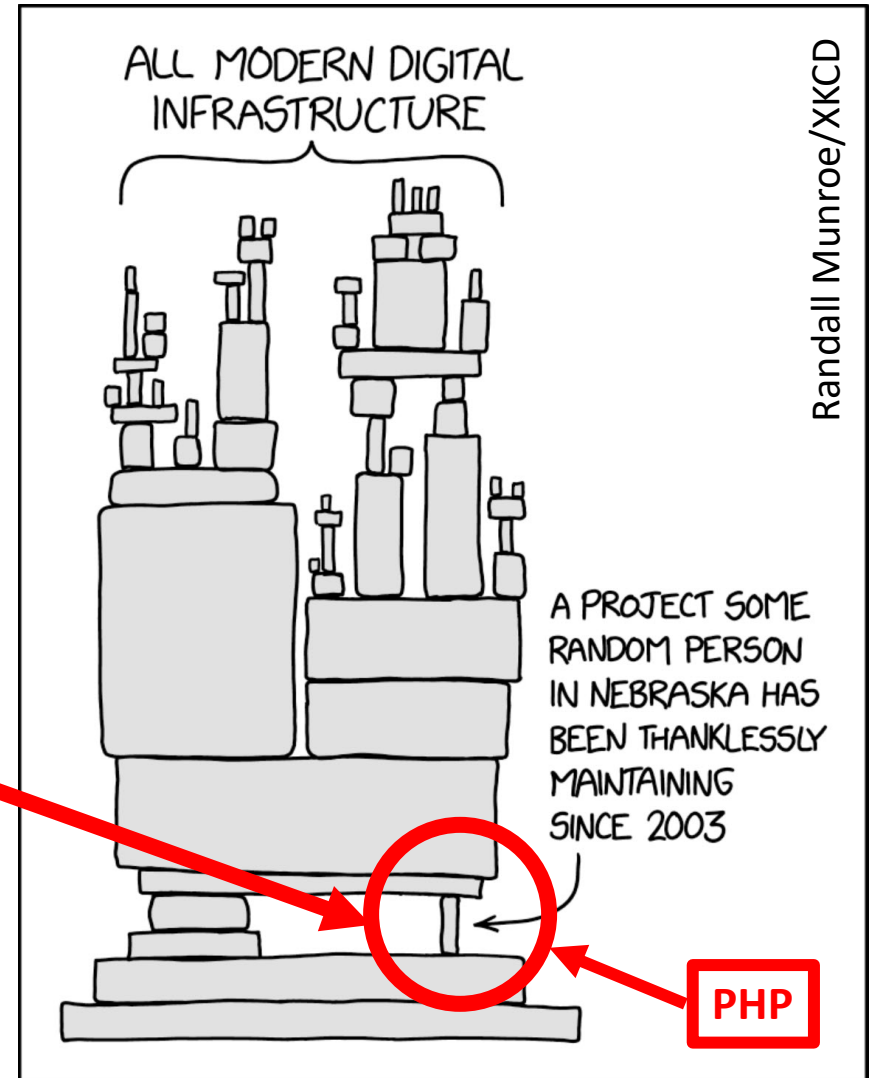
Sci-Fi?

- The great July hack – predicted last year
- From lethal scare to *friendly artificial intelligence*?
- Computing security has just become much more complex
- If you are not the solution, you are the problem



Not Sci-Fi

- The PHP scare of 2026
- PHP runs on 69% of all websites
- Thousands of servers shut down globally last week
- *No time to ponder, must act*
- Level 9.2–10 vulnerabilities was discovered using AI
- PHP has 13(!) employees
- Cybersecurity is now a whole new ballgame





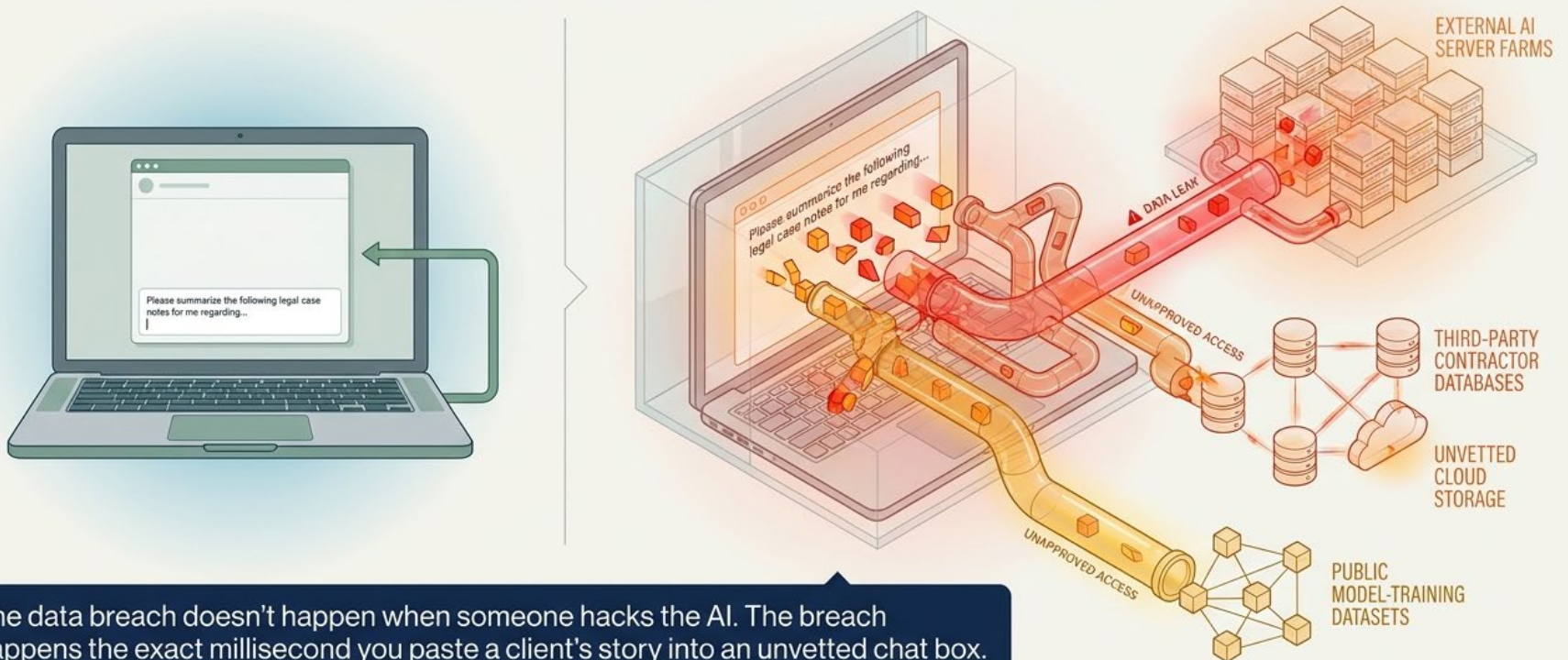
An Expanded View on Security and Information Protection

- Threats and Protections: An AI story
- AI Tools Contracted by Rutgers
- AI at SSW
- Plans
- “Old-fashioned” Computing Security



THE INVISIBLE BREACH: PROTECTING UNIVERSITY & CLIENT DATA IN THE AGE OF AI

Why the moment you hit “send” matters more than the AI’s answer.

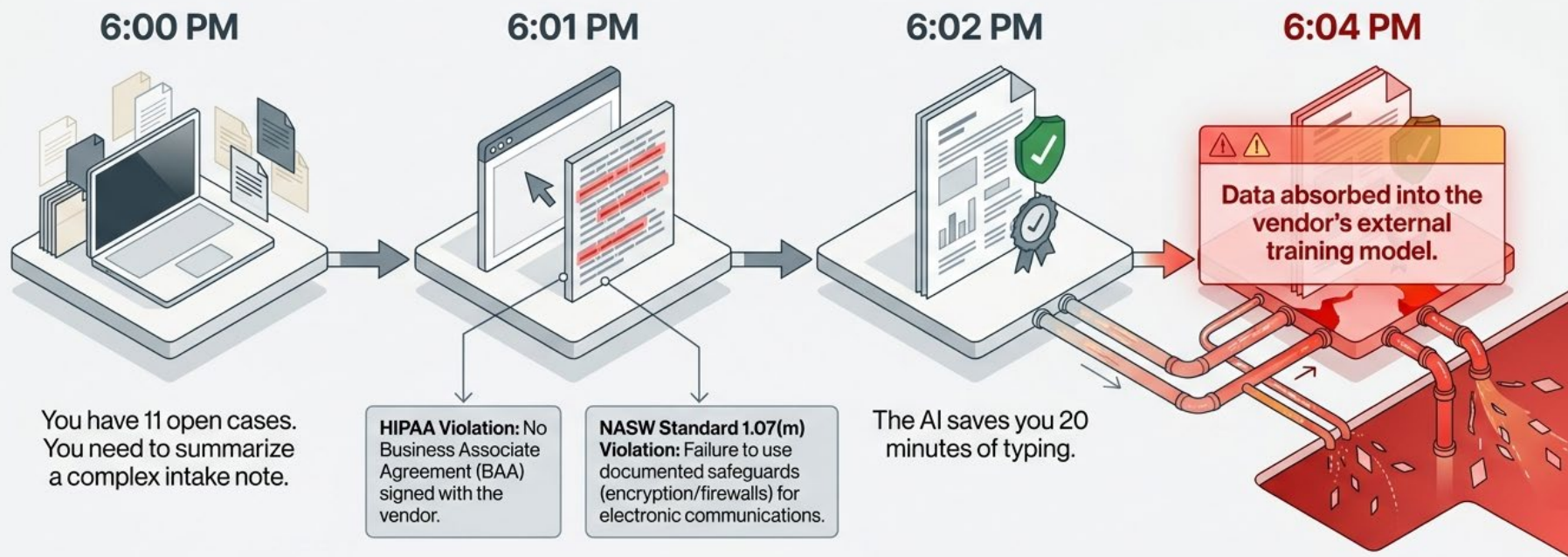


The data breach doesn't happen when someone hacks the AI. The breach happens the exact millisecond you paste a client's story into an unvetted chat box.



A Hypothetical Scenario

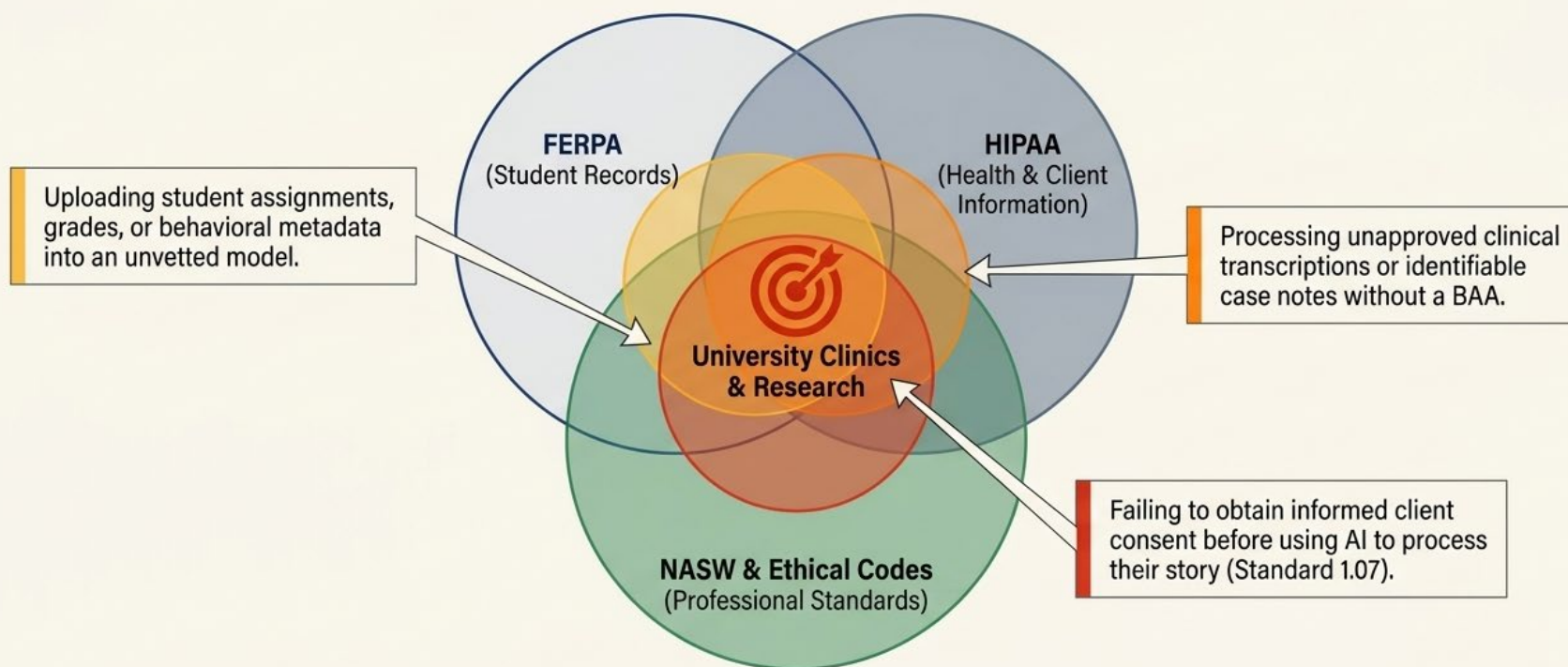
The 6:00 PM Mistake: The Breach is the Disclosure, Not the Summary



Removing a name isn't enough. Specific narratives—rare diagnoses, exact addresses, unique family situations—are still highly identifiable.



The Multi-Layered Risk of University Data



Universities handle a highly mixed data estate. A single casual prompt—like asking a public bot to transcribe a clinical supervision meeting—can simultaneously violate federal law, student privacy, and professional licensure ethics.



The 4-Step Safe Workflow



You can use AI to work faster, but if you wouldn't hand the text to a stranger on the street, don't paste it into a public bot.



The Architecture of Exposure: Where Does the Story Go?

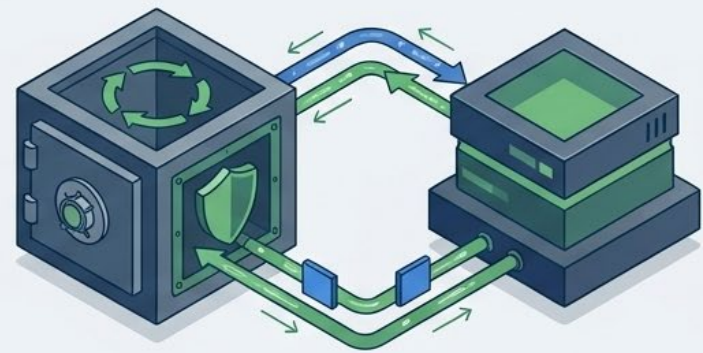
AI is not banned. Unmanaged data destinations are.

Consumer AI (Free Tiers, Unvetted Extensions)



Data Agreement:	None.
Data Retention:	Stored indefinitely on external, unmonitored servers.
Model Training:	Your client data trains their future models.
Institutional Control:	Zero.

University-Approved AI (Enterprise/Protected Tiers)



Data Agreement:	Legally binding Business Associate Agreement (BAA) / Data Protection Addendum.
Data Retention:	Minimal retention; auto-deleted after the session ends.
Model Training:	Segregated. Zero training on your inputs.
Institutional Control:	Managed entirely by University IT.

The ethical line is not the tool itself, but who controls the data after you press send.



AI Tools Contracted by Rutgers

- Where to look: it.rutgers.edu/ai/
- Some available w/o additional cost
- Higher-level tools available via subscription
 - Or based on per-usage fees
- Built-in AI tools
- Relevant usage policies
- Frequently changing environment



Centrally Financed Tools

- Microsoft Copilot Chat
- Google Gemini
- Gemini Notebook

Tools Built into Applications

- Zoom AI Companion
- Adobe Express AI
- AI-powered Coaching in LinkedIn
- Grammarly for Education



RU AI Tools for a Subscription Fee

- Must be purchased individually per Rutgers Connect account
 - [Microsoft 365 Copilot](#) (tied to MS365 tools)
 - [ChatGPT Edu](#)
- Subscriptions through ScarletMail accounts
 - [Google AI Pro](#)
- [Claude Premium coming]



New Rates for Chat GPT

Rutgers ChatGPT Tenant				
ChatGPT	ChatGPT Pro	HIPAA	HIPAA Pro	Research
Base \$10	Pro \$200	Base \$10	Pro \$200	Pro
Standard \$30		Standard \$30		



Expected Rates for Claude

Rutgers Anthropic Tenant

Claude

Standard

\$20

Premium

\$50

HIPAA

Standard

\$20

Premium

\$50



Portkey (LLM Access, Per-usage Fee)

- RU's enterprise AI gateway to multiple LLMs
 - GPT, Claude, Llama, and many others
- Single, unified API that SSW IT manages for all SSW projects
- Programmatic access to AI models
 - Build AI-powered applications
 - Integrate AI into workflows
 - Explore AI in computational courses
 - Automate tasks with scripts or code



How Portkey Works

- Unified API (Get API key from SSW IT)
- Data protection and access control
 - RU data not used for model training
 - But DO NOT send PHI
 - Internal information security level only (Policy 70.1.2)
- Cost tracking and monitoring
- Pay for the model you use, based on usage
 - Rates vary by model
- Monthly payments through your GL string



AI at SSW

- Several initiatives in progress
 - Intranet chatbot
 - Project workflow agent (Hub for Aging Collab)
 - Travel Agent or “Conquer Concur”
- What if you need unapproved tools?
 - Third-party Risk Assessment
- What’s NOT included in RU AI tools
 - Shared agents



Plans

- Please let SSW IT know of your plans and needs for AI tools
- Survey on AI usage and needs at SSW coming
- Working on a procedure how to reach non-university AI tool usage agreements



Email Security 1/2

- Phishing: Increasingly prevalent and convincing
 - Sent from non-Rutgers email domains
 - E.g., sswdean@gmail.com
 - Sent from a compromised email account belonging to a legitimate Rutgers user or legitimate business partner
 - e.g. person@rutgers.edu or person@nj.gov
- Judging legitimacy: Normal behavior for this sender?
 - Context: Did you *expect* to receive an unsolicited password-protected Excel document without explanation?
 - Classic signs: urgency, authority, unused services, spelling or grammar issues



Email Security 2/2

- Avoid malicious hyperlinks
 - Check destination by hovering over URL before clicking
 - Be cautious of shortened links (tinyurl, bit.ly, etc).
 - <https://tinyurl.com/ssw>
 - Be cautious of QR codes from unknown senders
 - Contact the sender by phone to verify
- Contact IT@ssw.rutgers.edu
 - Include the suspected message as an attachment
 - Use “report phishing” function in Outlook



Additional Best Practices

- Avoid installing unverified browser extensions
- Download application installers from legitimate vendor websites
- Install Windows and macOS updates when prompted
- Update third-party applications when prompted
- Transition laptops/mobile devices to eduroam:
<https://it.rutgers.edu/wifi/>
 - RUWireless Secure decommissioned January 4, 2027



Thank you!
Questions?

If in doubt,
or in need of assistance:

it@ssw.rutgers.edu