The Prosperity Project

FEC & the Restricted Class

- Clearly defined audience for "advocacy" & "good government" messages
  - Managers, executives, shareholders
    - PAC solicitation, advocacy for candidates
  - All employees
    - Voter registration, voting records, grassroots involvement

- Penalties include substantial civil fines

BIPAC P2

States & the Restricted Class

- Each state regulates their own elections
  - Ranges from
    - Unlimited corporate contributions and advocacy
    - No corporate involvement whatsoever
- Penalties also vary
  - Most severe
    - Large personal fines for corporate officers
    - 10 Years jail time
    - Corporate charter is disolved

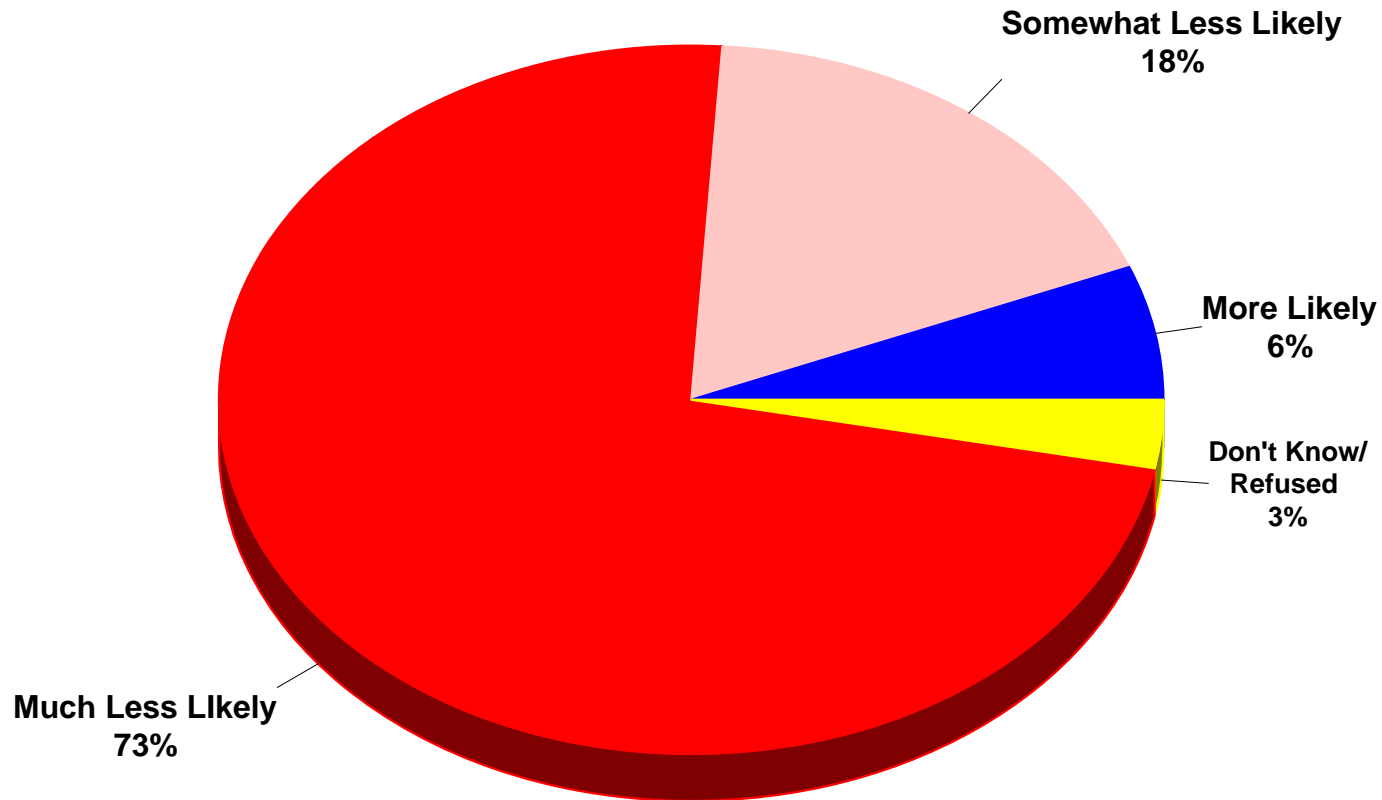# BIPAC's Goals for a Turnkey Solution

- Protect employee privacy

- Eliminate the need to give employee data to third-party vendors

- Provide information relevant to the employee without additional sign-on or registration

Without Liberty…

- Employers had these options
    - Do nothing – no political information shared with employees
    - Use paper-based communications only
    - Develop expensive in-house communications tools
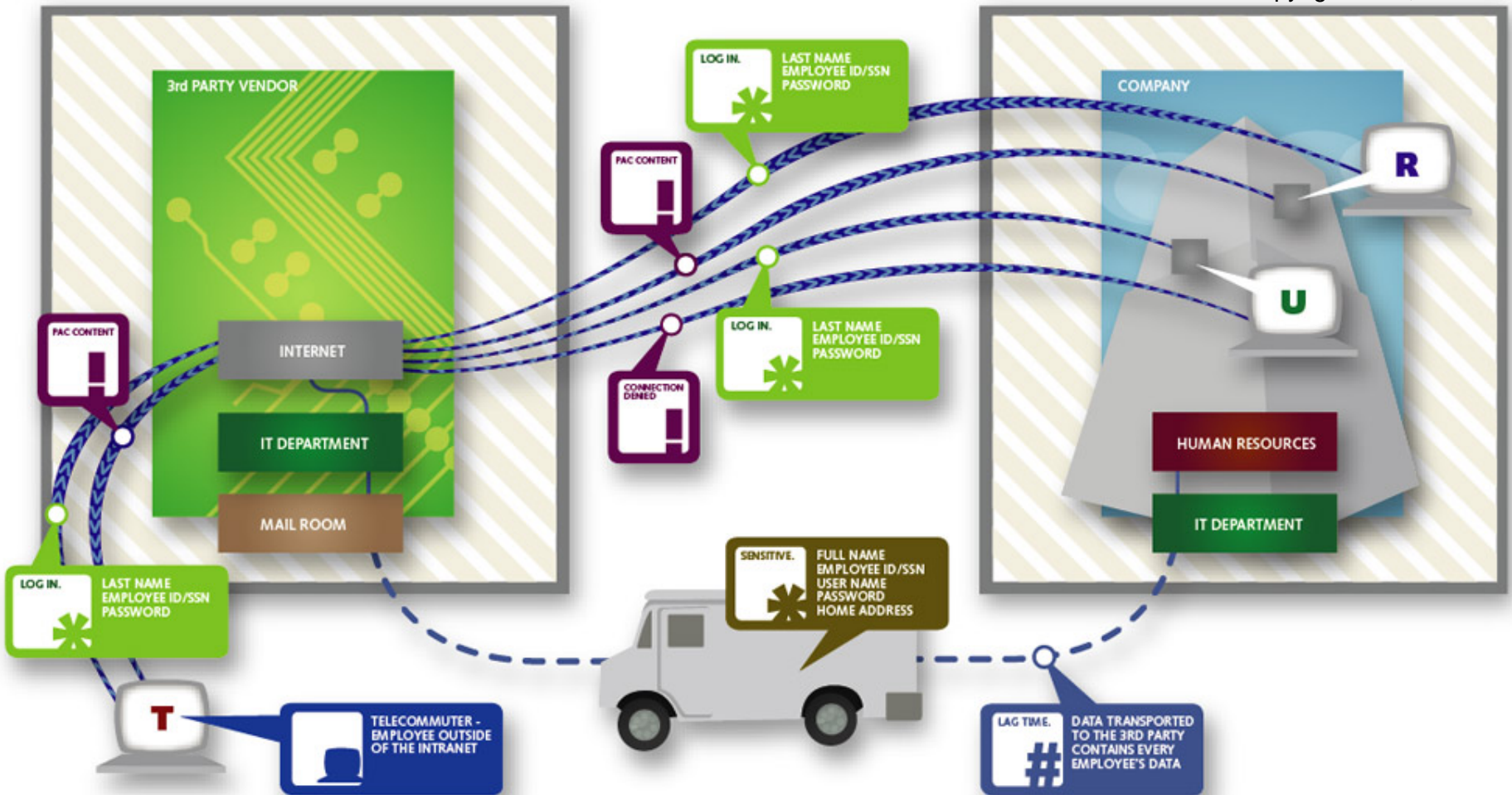   - Use third-party vendors to authenticate users and provide content

BIPAC **P2**

Turning Away 9 out of 10 Employees

"Would you be MORE LIKELY or LESS LIKELY to visit a website that requires you to register before you are allowed to view political or voter information?"
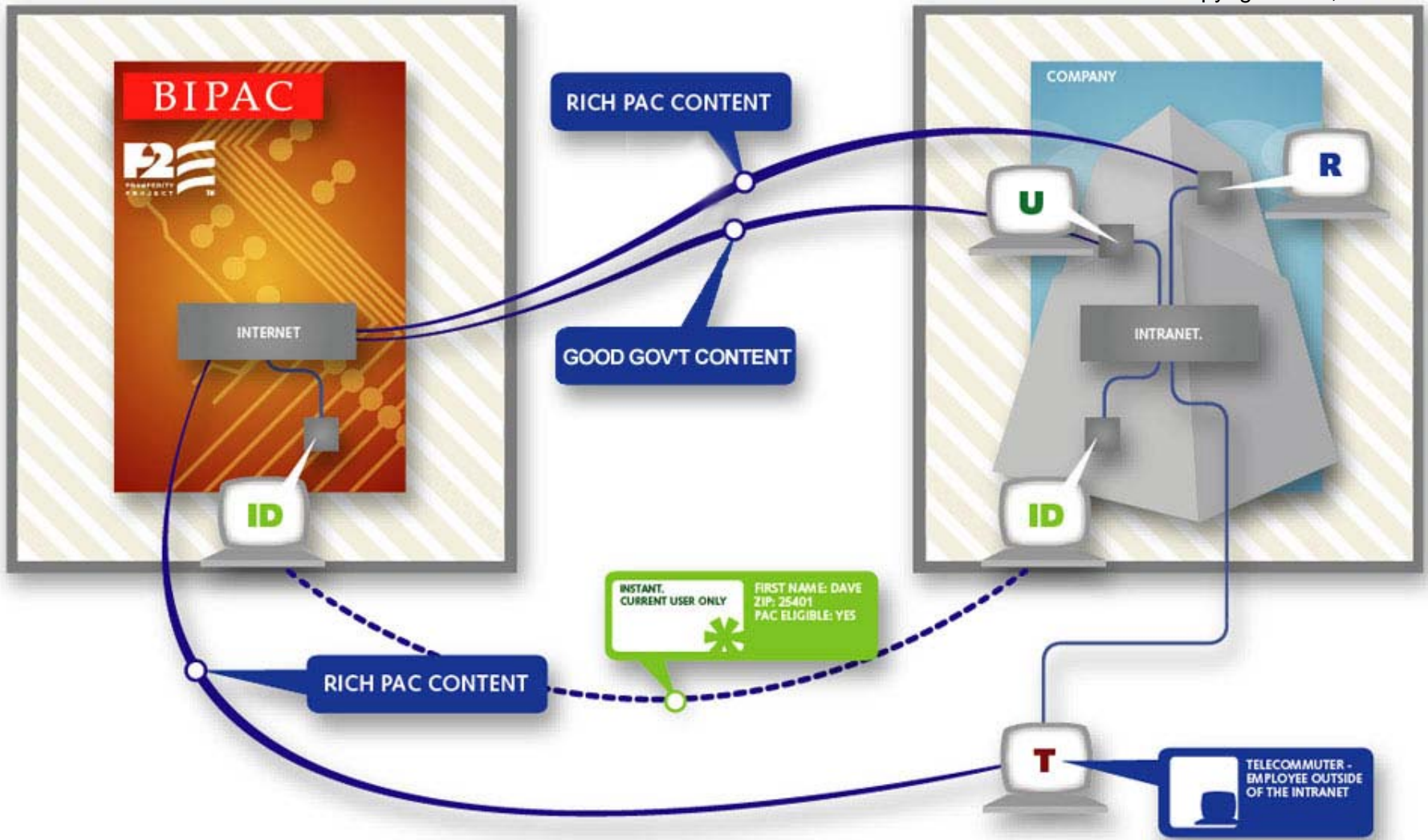

Somewhat Less Likely
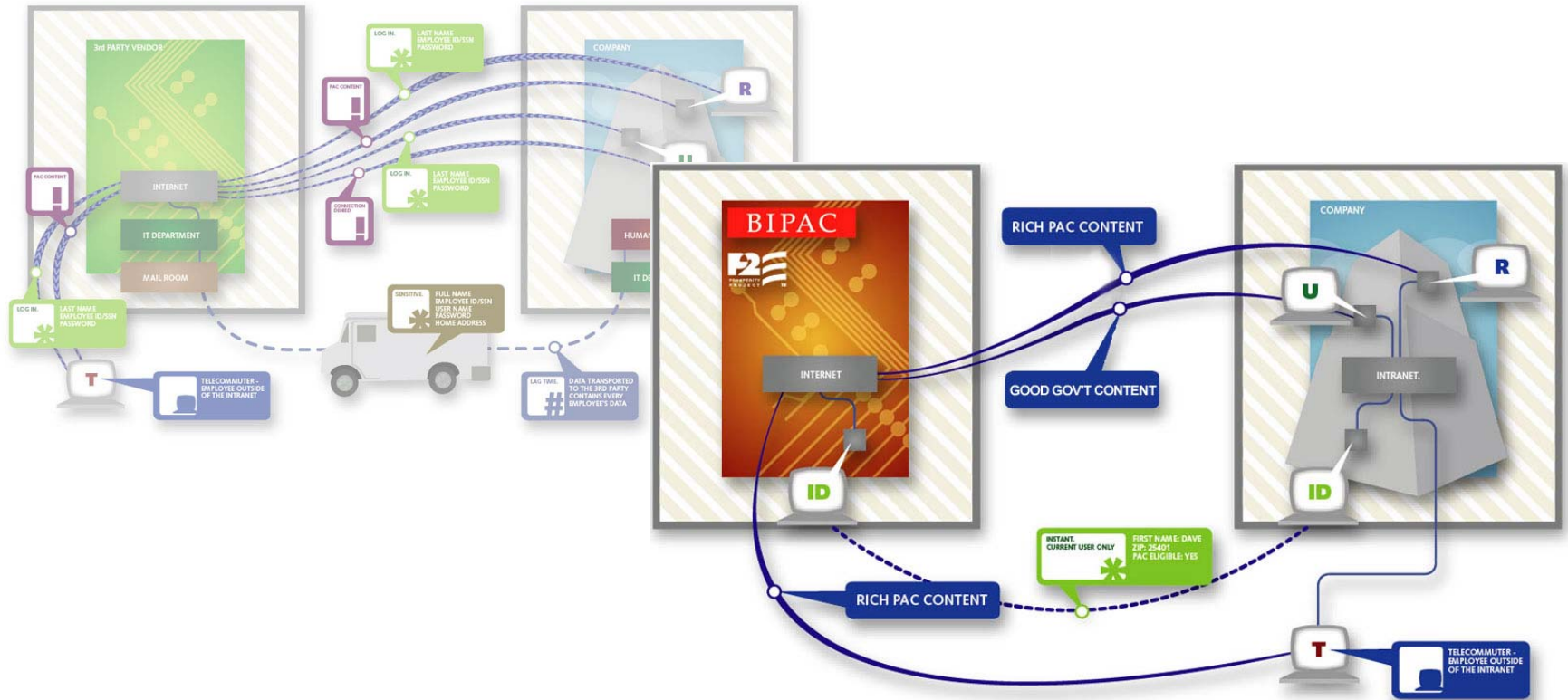**18%**

More Likely
6%

Don't Know/
Refused
3%

Much Less LIkely
73%

BIPAC P2E

Before...

After...

Benefits

The Liberty Alliance

Board and sponsor members include:

BIPAC and Sun Microsystems

Other Circle of Trust Models

User

Airline

Hotel

Service Providers

Identity Provider

Camp Reservation

Payment Service

Interaction Service
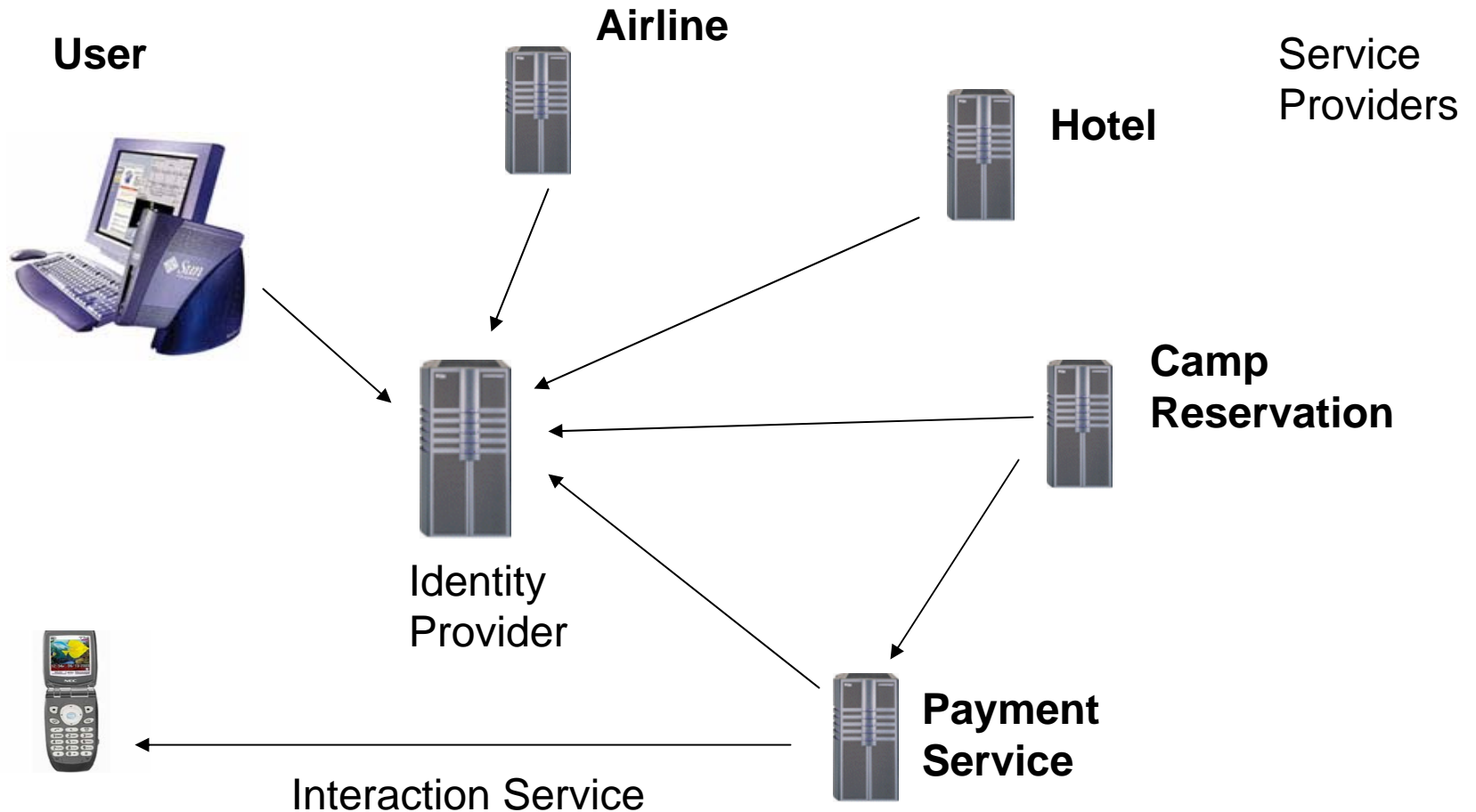
Liberty Id Theft Mitigations

- Fewer authentication points
  - Easier to 'get it right' in fewer places
  - Easier to implement stronger authentication and anti-phishing mechanisms in fewer places
  - Users more likely to recognize imposter sites
  - Fewer places to update credentials after breaches

BIPAC

Liberty Id Theft Mitigations

- **Information in fewer places**
  - With federation, less sensitive data shared
  - Information frequently identified differently at different sites – harder to correlate
  - Data from one service provider may not help at another
  - Ability to retrieve up-to-date information when you need it, then discard or rely on assertions

Liberty Id Theft Mitigations

- Hacking into systems/SQL injection
  - Less personal data at each service provider
  - Hackers get less information for their efforts
- Phishing
  - Fewer points to secure means easier to implement stronger authentication and anti-phishing mechanisms
- Social Engineering/Trusted insiders/Dumpsters
  - Information from one site doesn't necessarily help in attacking another site
  - Identity Providers likely to implement education against social engineering attacks

Liberty Id Theft Mitigations

- Screen Scraping/Spyware/Trojans
  - Best mitigation is anti-spyware
  - Fewer sites to update after a breach
  - Better visibility to detect different behavior
- Wardriving/sniffing..
  - Fewer authentication points means
  - Easier to ensure proper implementation
  - Proper use of encrypted communication

BIPAC

For More Information

p2@bipac.org   800-497-8351

BIPAC
888 16th St NW, Suite 305
Washington DC 20006