THE HARMS CAUSED BY PRIVACY VIOLATIONS

Attack trends on data breaches, medical identity theft, card-not-present fraud and responses from FTC and CNIL

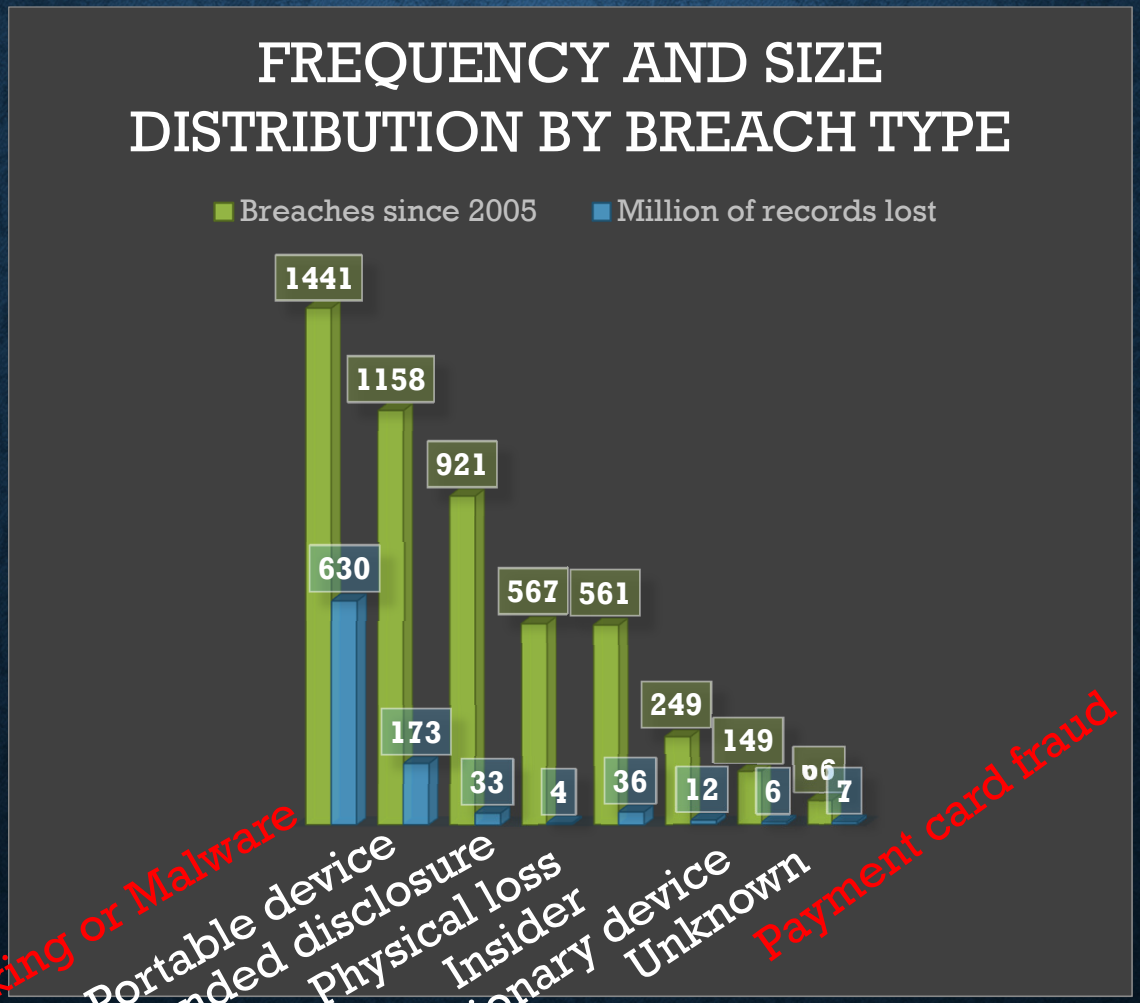
Empirical research funded by the National Science Foundation

Gwendolyn Lee & Ye Xia, University of Florida

PRESENTATION SUMMARY

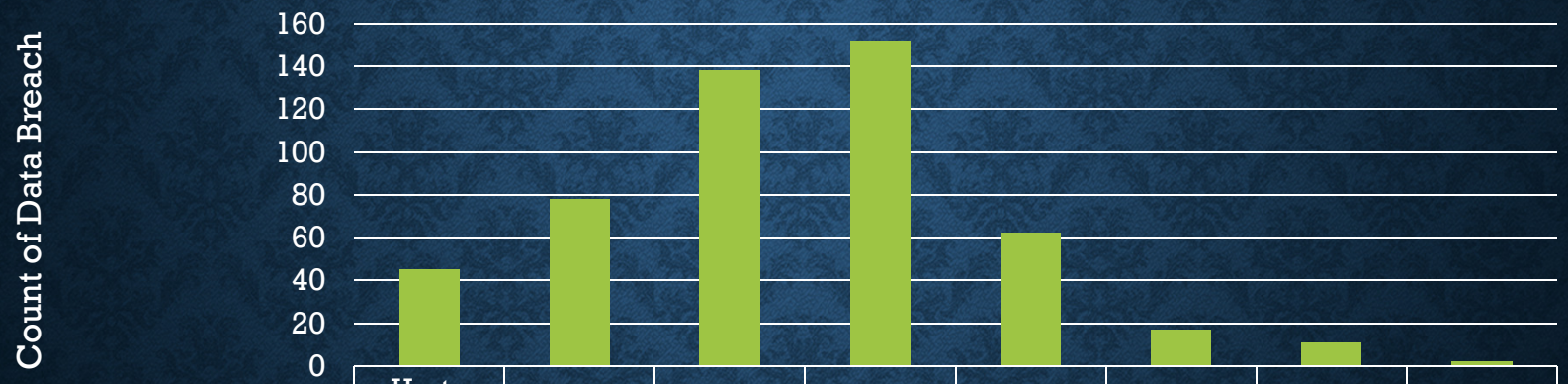
- **The harms caused by privacy violations** increase with widespread data breaches and security failures
  - The exposure of sensitive personal information leads to costly spam, phishing, and other unsolicited communications
  - The risks range from identity theft to "phantom debt" collection
  - Fraudulent purchases transacted with stolen information cause substantial injury, including inconvenience, worry, and time loss dealing with the affected credit/debit cards
- **Attack trends** show that
  - Hacking or Malware is the leading type of data breach
  - A small number of breaches accounts for a large proportion of the records lost
  - Healthcare, education & businesses are the leading entities suffering the most data breach
  - Electronic devices (portable and stationary) represent the leading source of data breach in healthcare
  - Illegally obtained account information across many states heightens the risk for unauthorized use and card-not-present fraud
- **Responses from government agencies** provide crucial enforcement actions
  - Compared to CNIL sanctions, FTC actions cover more companies across different industries involving a wider range of privacy practices.

HACKING OR MALWARE IS THE LEADING TYPE OF DATA BREACH



HACKING OR MALWARE IS WIDESPREAD, HURTING USERS SUCH AS THE HALF-A-BILLION USING YAHOO!

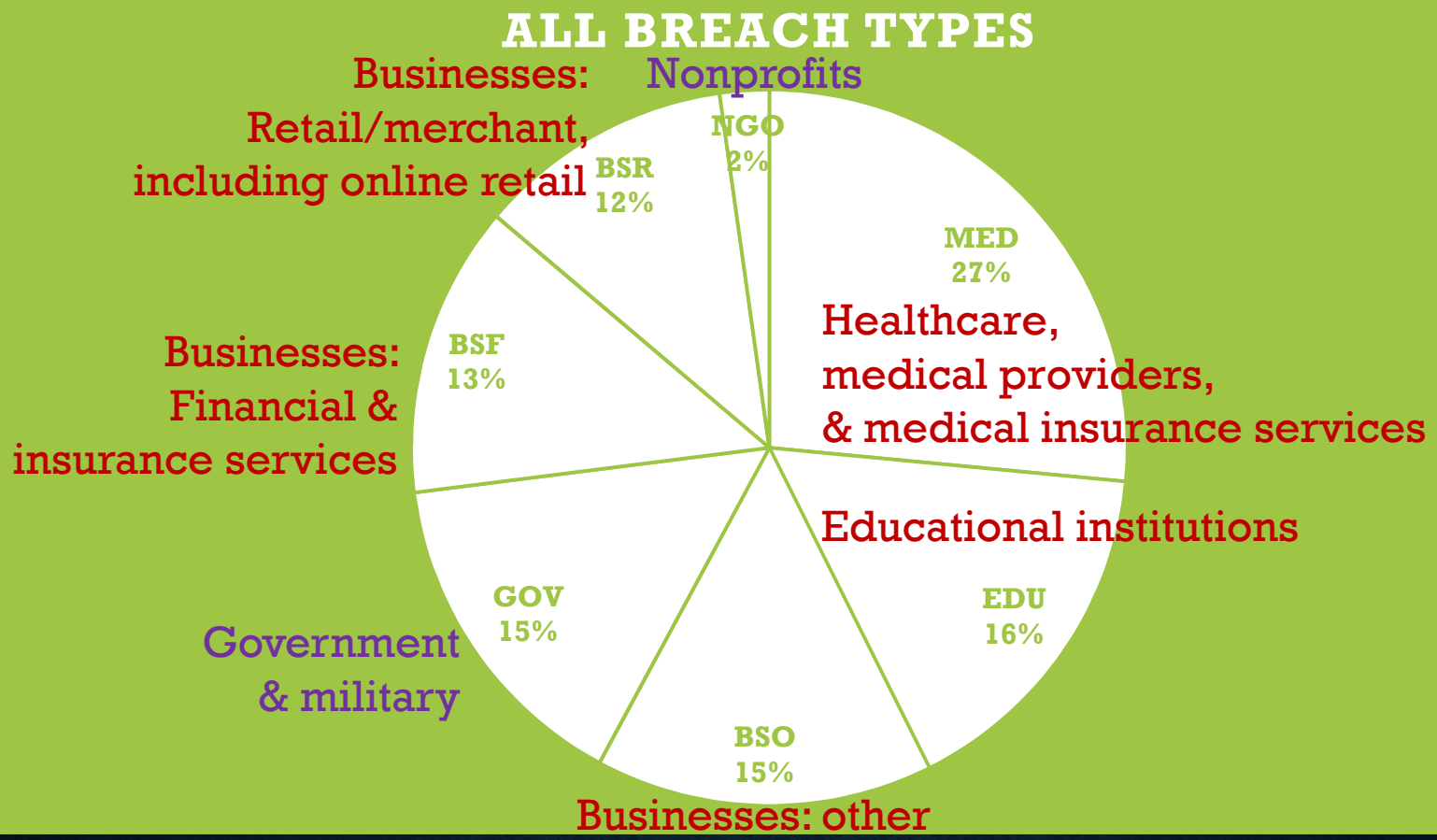
Skewed distribution: A small number of breaches accounts for a large proportion of the records lost



	Up to 100 records lost per breach	1,000	10,000	100,000	1 MM	10 MM	100 MM	Greater than 100 MM
Hacking or Malware	45	78	138	152	62	17	11	2

Yahoo! acknowledged that a state-sponsored attack in 2014 stole the following user account information: names, email addresses, telephone numbers, dates of birth, hashed passwords and, in some cases, encrypted or unencrypted security questions and answers.

HEALTHCARE, EDUCATION & BUSINESSES ARE THE LEADING ENTITIES SUFFERING THE MOST DATA BREACH



MEDICAL IDENTITY THEFT

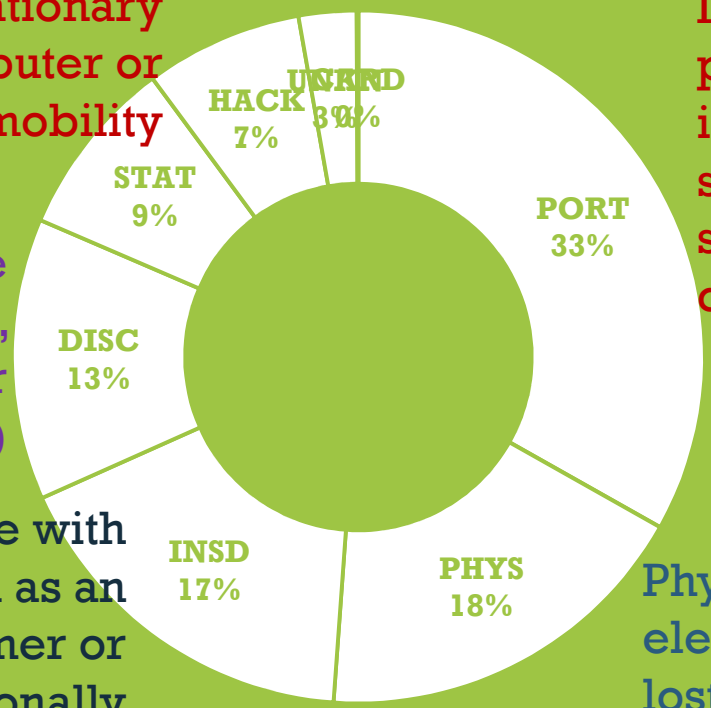
Electronic devices (portable and stationary) represent the leading source of data breach in healthcare *, not hacking or malware, which is the leading type of data breach when all industries are combined in the analysis*

DATA BREACHES IN HEALTHCARE

Lost, inappropriately accessed, discarded or stolen stationary device such as computer or server not designed for mobility

Unintended disclosure (not involving hacking, intentional breach or physical loss)

Insider, someone with legitimate access—such as an employee, customer or contractor—intentionally breaching information

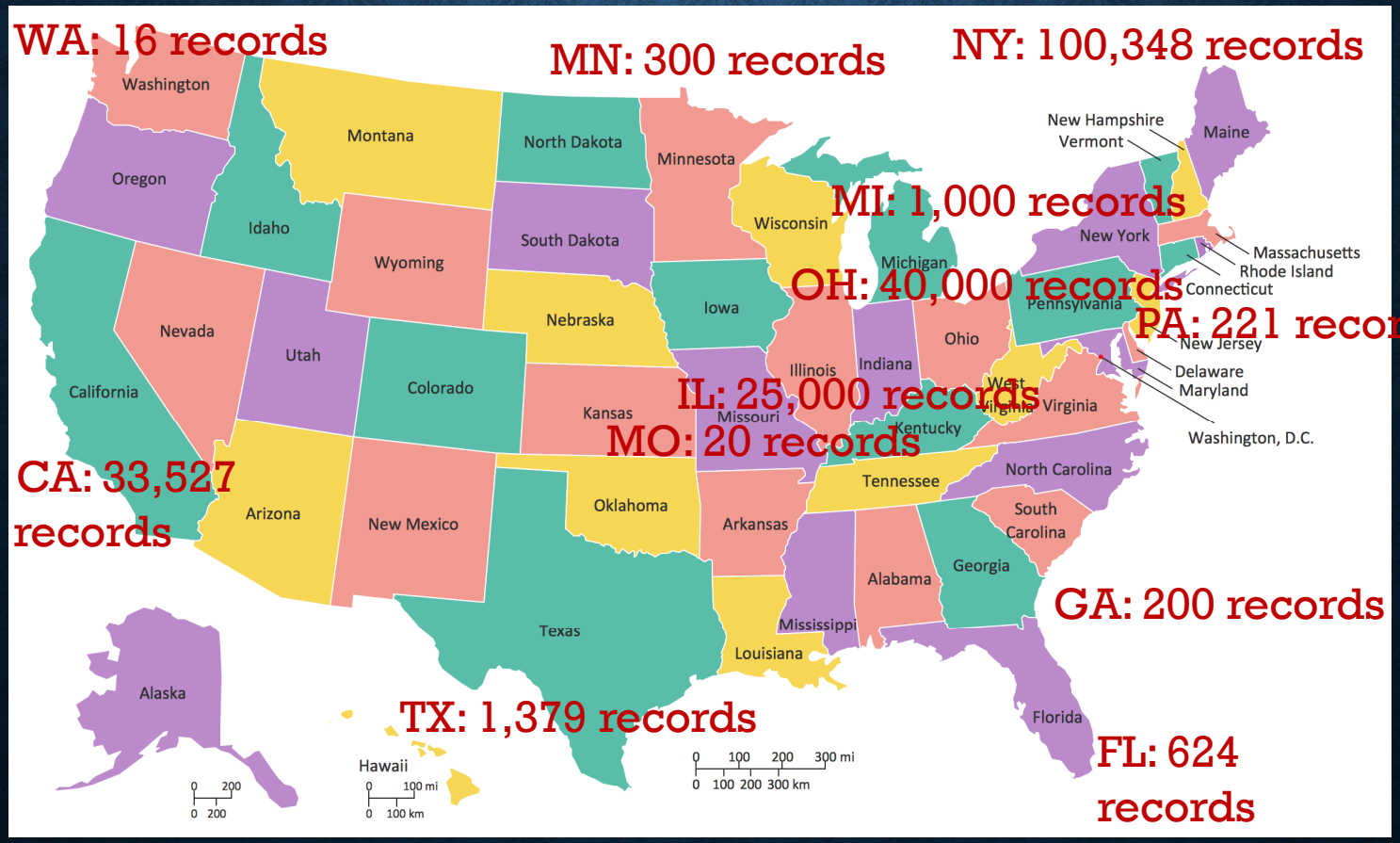


Lost, discarded or stolen portable devices, including laptop, PDA, smartphone, memory stick, CDs, hard drive, data tape, etc.

Physical loss from non-electronic sources that are lost, discarded or stolen, including paper documents

CARD-NOT-PRESENT FRAUD

Illegally obtained account information across many states heightens the risk for unauthorized use and card-not-present fraud



RESPONSES BY GOVERNMENT AGENCIES

USA vs. France on government responses to data breach and security failure

- FTC cases on data security and information exposed, 2005 - 2016
  - Privacy violation: Unauthorized access
    - Failures to protect sensitive information, including personal, financial, health, and employment data as well as video content from **Internet of Things**
  - Privacy violation: Identity theft
  - Privacy violation: Card-not-present fraud
    - Fraudulent purchases transacted with stolen information, causing substantial injury including inconvenience, worry, and time loss dealing with the affected credit/debit cards
- CNIL sanctions in France, 2006-2015
  - Privacy violation: Cyber surveillance security failures
  - Privacy violation: Video surveillance security failures
  - Privacy violation: Data breach and security failures

FTC ENFORCEMENT ACTIONS

Privacy violations are caused by failures of companies across different industries involving a wide range of privacy practices.

Unauthorized access caused by

- Social network operators: Twitter, Snapchat
- Social game operator: RockYou
- Internet of Things marketer: TRENDnet
- Consumer electronics companies ASUSTek, Compgeeks
- Software developer: Guidance Software
- Retailers Life is good, Petco Animal Supplies
- Debt collector EPN
- Debt brokers Bayview and Cornerstone
- Mortgage broker Gregory Navone, Mortgage lenders JBN, Premier Capital Lending
- Real estate services company Nations Title Agency
- Student loan lender Goal Financial
- Credit report resellers ACRAnet, SettlementOne, and Statewide Credit Services

Identity theft caused by

- Data broker ChoicePoint
- Consumer reporting agency Rental Research Services

Exposure of medical and insurance info caused by

- Healthcare industry value chain: LabMD, GMR Transcription Services, Accretive Health, CVS Caremark, Rite Aid

Card-not-present fraud caused by

- Credit card processor CardSystems Solutions
- Data brokers Reed Elsevier and Seisint
- Entertainment operator Dave & Buster's
- Retailers TJX, BJ's Wholesale Club, Shoe discounter DSW

CNIL SANCTIONS

Privacy violations are caused by failures of companies and public establishments

Cyber surveillance

security flaw

- Un named public establishment

Failure to respect privacy and individual freedoms & failure to perform a lawful and fair collection of data

- Google

Video surveillance

failing to ensure data security

- New Telephone Communication
- Professional Service Consulting
- Sports Federation
- JEAN MARC PHILIPPE, ready-to-wear company, specializing in the creation of large size

Data breach & security failure

- Telecommunication service provider ORANGE
- Luxury vehicles leasing company DREAM CAR
- Transport business, logistics and freight company DHL International Express France

Telecommunication Service Provider Orange: a server malfunction led to a breach of personal data, compromising 1,340,000 mobile phone customers' name, date of birth, email address, and phone number.

INFORMATION SOURCES

We are grateful to the following information sources
for sharing valuable data

- FTC
- CNIL
- Privacy Rights Clearinghouse, 2005 through September, 2016
- Media
- Attorney general
- Government agencies,
- Dataloss database
- Databreaches.net
- Privacy.net