IMAGINE THE POSSIBILITIES...
Fraud Prevention and Privacy Law: Emerging Conflicts Between Privacy Law and Fraud Prevention

Will Bracker
Corporate Counsel, Privacy
Cox Communications
Will.Bracker@cox.com
Overview

Introduction
Comprehensive Privacy Laws: a new era
Privacy law and fraud
Conclusion
Introduction

Handful of existing CPLs
- GDPR
- CCPA
- PIPEDA
- More coming…

Privacy laws may impact how you identify, mitigate, and prosecute fraud

Source: US State Comprehensive Privacy Laws, IAPP, online.
Comprehensive privacy legislation elements are broken into two broad categories: **consumer rights** and **business obligations**.

**Consumer rights** attempt to give citizens greater control over the **collection and use** of their personal data as well as **legal recourse** for misuse or loss.

**Business obligations** are **new compliance requirements** surrounding the collection and use of personal data.

### Consumer Rights
- Access to collected data
- Access to shared data
- Correct data
- Delete data
- Restrict use
- Portability
- Opt-out of use
- Prohibit automated decision making
- Private right of action

### Business Obligations
- Age based opt-in
- Notice/Transparency requirement
- Data breach notification
- Risk assessment
- Prohibition on discrimination
- Purpose limitation
- Processing limitation
- Fiduciary duty
Compliance Challenges

- Definitions differ
- Complex requirements
- Business impacts
- Short timelines
- Serious penalties
The new laws create challenges for companies and opportunities for fraudsters

Weaponizing the Right to Know

- The right to know can be used by bad actors to gather personal information of their targets
- Using GDPR requests and publicly available information, a security engineer was able to gain credit card numbers, educational records, login credentials, dating profiles, hotel and travel records

Blackhat 2019

- GDPRarrrr: Using Privacy to Steal Identities
- Pavur and Knerr
Privacy law and fraud prevention

The new laws create challenges for companies and opportunities for fraudsters

Weaponizing the Right to Be Forgotten

- Fraud detection uses past actions and activity to estimate the risk of a transaction
- Aware of this, individuals who have previously engaged in fraudulent activity have made GDPR right to be forgotten requests to have the records of their activity expunged
- Although an exception to the right exists in the regulation, that has not prevented companies from honoring the requests
The influx of money from COVID-19 relief programs combined with the new contactless digital society has created new opportunities for fraudsters.

Weaponizing the Right to Know

- In a sixteen week period, $108 million in COVID related fraud was reported to the FTC
- Exception processing that used to end in physical presentation of self and picture ID is no longer feasible
- Distanced communications channels have complicated the investigative process as well
Thank You!

Will Bracker
Corporate Counsel, Privacy
Cox Communications
Will.Bracker@cox.com

Simon Krauss
Deputy General Counsel
CableLabs
s.krauss@cablelabs.com

Steve Goeringer
Distinguished Technologist
CableLabs
s.goeringer@cablelabs.com