Privacy & security policy considerations for mobile payments & digital currency

October 14, 2014

Harley Geiger
Senior Counsel
@HarleyGeiger

CDT.org

- Global nonprofit focused on technology and civil liberties.
- Privacy, free expression, Internet governance, innovation, and human rights.

KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

Mobile Payments & Digital Currency

- The future!
- Big business!
  - Many major companies involved.
  - Gartner forecast 35% annual growth for mobile payments 2012-2017.
  - Growing acceptance of digital currency.
- Now is the time to ensure privacy & security are protected.

Mobile Payments

- Barriers to adoption
  - Infrastructure
  - Privacy, Security, Convenience
- Bain, 2014: Privacy, security, convenience holds back 80% of US/EU consumers.
- Accenture, 2013: 45% North American smartphone users concerned with mobile payment security, 37% with privacy.

Privacy

- Mobile payments can provide more user data to more entities.

	Traditional Payments (Credit, etc.)	Mobile Payments
Merchants	Collect data on specific purchases ("Level 3" data, SKU), but not customer contact info.	Can collect data on specific purchases, customer contact info, link to previous purchases and customer profile. Loyalty programs.
Payment network	Collect purchase charge, merchant identity, but not specific purchases. Already have customer contact info.	Can collect purchase charge, merchant identity, specific purchases, link to previous purchases and profile. Maintain contact info.

Privacy

- Berkeley, 2012:
  - 81% of American consumers object to transfer of telephone number to merchant when using mobile payments;
  - 81% object to transfer of physical address;
  - 51% object to transfer of email address.
- When is informed consent given? Express, implied, opt-in? Once, or with each purchase?
- What choices do consumers have to share or withhold this information?

Security

- Currently not very good for traditional payments.
- Security depends on more actors with mobile payments.
- More sensitive data = greater severity of data breach.
  - Ponemon, 2014: Average cost of data breach is 3.5 million USD. Plus loss of customer loyalty.
- Man-in-the-middle. Malware.

Fair Information Practices

- Transparency
- Individual Participation
- Purpose Specification
- Data Minimization
- Use Limitation
- Data Quality and Integrity
- Security
- Accountability

Privacy Recommendations

- Regulators should ensure existing consumer protections are adequate.
- "Privacy by design."
- Merchants & service providers should specify how they will use data at POS.
- Merchants should not require that users download content not directly related to purchase.

Privacy Recommendations

- Collecting and sharing limited data aids consumer privacy and convenience, and reduces security risks for businesses.
- Merchants & service providers should preserve the ability to withhold data.
- Merchant-facing: Allow consumers to withhold data not necessary to transaction.
- Wallet-facing: Allow consumers to withhold sharing purchase information.

Security Recommendations

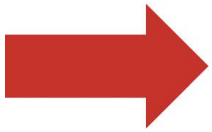
- Secure multiple points of risk, including customer information in transit & storage.
- Point of Sale system security software & audits.
- Store payment data locally on device within secure element, authenticate transactions (chip & pin).
- One-time transaction ID tied to fixed sum.

Cryptocurrency

- Money or good?
- Potential to bank the unbanked, streamline financial services (inc. remittances), hedge against fiat.
- Value can fluctuate, backed by trust, and has privacy-enhancing properties.
  - …just like cash.
- Decentralized, peer-to-peer global transactions.

Cryptocurrency recommendations

- Preserve financial privacy for most transactions.
  - Potential exceptions: large sum, high-risk goods.
- Focus identity regulations on exchanges.
- Minimize regulations for user-controlled wallets.
  - Focus on wallets with custodial control.
  - Focus on cybersecurity, user privacy.



Thank you!

Harley Geiger

Senior Counsel, CDT

@HarleyGeiger

cdt.org

KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE