Texas A&M University School of Law

From the SelectedWorks of Mark Edwin Burge

April 18, 2016

On the Regulatory Frontier: Developing Insights From Payment Transactions

Jason Korosec
Mark Edwin Burge, Texas A&M University School of Law
David P. Stewart, Georgetown University Law Center

Available at: https://works.bepress.com/mark_burge/20/
On the Regulatory Frontier: Developing Insights from Payment Transactions

**Jason Korosec**
- Group Head & Senior V.P. for Business Intelligence
  MasterCard Advisors

**Mark Edwin Burge**
- Associate Professor of Law
  Texas A&M University School of Law

**David P. Stewart**
- Professor from Practice
  Georgetown University Law Center
Developing Insights

Exploration of how transaction data can drive insights using anonymous, aggregated, and cleansed data

Jason Korosec
Adjunct Professor
Texas A&M University
School of Law

Adjunct Professor
Case Western Reserve University
School of Law

Group Head
MasterCard Advisors

Linkedin.com/in/jasonkorosec
@thepaymentsguy
ISO 8583 Transaction Example

Cleansing and aggregation critical to deriving value
Mapping Insights to Data

By ticket size, total spend, frequency
“Locals” or “Visitors/Tourists” purchase patterns
Work or Home
Purchase loyalty
Preference for Hilton
Preference for Italian
Level
By segment / cluster
By Geography

Category

Purchase Patterns

Purchase periodicity
By geo / demo
By time / day / month
By category / industry / merchant
By online / offline

Purchase sequencing
People that shop here tend to then go here next
Sequence by merchant
Sequence by merchant / time
Sequence by merchant / geo

People that shop at these three merchants also shop here

Purchase affinities

Market

Purchase propensities
Are you likely to be interested in this merchant or category?
How much will you spend?
How often will you spend?
Look a like
People that look like me also like to shop here

Geo / demo
Purchase patterns

Mapping Insights to Data

Purchase pizza every Friday
Skiing vacation every January
Vacation every spring break
Back to school shopping every year at Retailers
By time / day / month
By location
People that shop here tend to then go here next
Sequence by merchant
Sequence by merchant / time
Sequence by merchant / geo
People that shop at these three merchants also shop here
Insights by business need

- **Market intelligence**: What are market and sector trends that could affect your business?
- **Business intelligence**: How is your business performing?
- **Customer intelligence**: How can you grow your business through better engagement of existing and new customers?
- **Location intelligence**: Where should you go, buy or locate?
- **Operational intelligence**: How can you improve operations and business efficiency?
Local Market Intelligence

**Small Business Case Study**

How is my business performing?
- Key performance metrics, with benchmarks
- Analytics drive client decisions through question, answer, and recommended action

How loyal are my customers?
- Insights into customer loyalty, purchase frequency

How can I get more customers?
- Deeper insights into customer information
  - Feeder geographies with competitor insights
  - Segmentations
  - Day of Week & Time of Day analytics
Navigating the Frontier

Regulatory Rumblings on the Domestic Front

Mark Edwin Burge
Associate Professor of Law
Texas A&M University School of Law
Fort Worth, Texas
CFPB’s Vision of Consumer Protection in New Faster Payment Systems (July 9, 2015)

- Prepared in the wake of various faster payment system initiatives, including efforts by NACHA and the Federal Reserve.

- Purpose: “[T]o facilitate the integration of consumer interests” into developing payment systems.

- “[W]e are not specifying how they must be achieved.”
Principle 2: Data and Privacy

“When helpful to consumers, consumers are informed of how their data are being transferred through any new payment system, including what data are being transferred, who has access to them, how that data can be used, and potential risks. As appropriate, the systems allow consumers to specify what data can be transferred and whether third parties can access that data. When consumer data are collected, they are only used in ways that benefit consumers. The systems protect against misuse of the data associated with payment transactions.”
“[O]ur public enforcement actions have been marked by orders, whether entered by our agency or by a court, which specify the facts and the resulting legal conclusions. These orders provide detailed guidance for compliance officers across the marketplace about how they should regard similar practices at their own institutions.”
“Some have criticized this approach as regulation by enforcement, but I think that criticism is badly misplaced. Certainly any responsible official or agency charged with enforcing the law is bound to . . . develop a thoughtful strategy for how to deploy their limited resources most efficiently to protect the public.

That means working toward a pattern of actions that conveys an intelligible direction to the marketplace, so as to create deterrence that can be readily understood and implemented.”
“Enforcement is the lynchpin of the FTC’s approach to privacy protection. To date, the FTC has brought over 500 cases protecting the privacy and security of consumer information. … The FTC’s enforcement actions—in both the physical and digital worlds—send an important message to companies about the need to protect consumer privacy.”
Meanwhile, Outside of Payments…

“Simply by using the Internet, you have no choice but to share large amounts of personal information with your broadband provider. You have a right to know what information is being collected about you and how that information is being used. That’s why establishing baseline privacy standards for ISPs is a commonsense idea whose time has come. The bottom line is that it’s your data. How it’s used and shared should be your choice.”

Federal Communications Commission Chairman
Tom Wheeler
March 10, 2016
Source: http://recode.net/2016/03/10/its-your-data-empowering-consumers-to-protect-their-privacy-on-broadband-networks/
Dominant Regulatory Approach:

- Reactive Enforcement – Public Examples

Industry Best Practices:

- Proactive Protection of Users – Transparent Disclosures with Available Opt-out when Data Collection is Non-anonymized
- “Creepy Test”
Privacy, Data Protection and Consumer Protection in the Transborder Context

David P. Stewart
Professor from Practice
Georgetown University Law Center
Washington D.C.
Privacy

- A Right to Privacy is recognized and respected in almost all legal systems around the world
- But “privacy” is defined differently in different legal systems
- In many foreign countries, the definition is broader than in the United States
Regulation

• In many foreign countries, “personal data” is given a wider definition and greater legal protection than in the United States.

• Many countries have broad national legislation protecting privacy and centralized enforcement mechanisms ("privacy/data protection agencies").
Cross-border Data Flows

- National regimes regulating privacy and protecting personal data increasingly apply to cross-border data flows.
- This means that personal data collected abroad and brought to the United States may be covered by the foreign rules.
Major Challenges

- Technological advances (electronic communications, cellular and internet connectivity)
- Globalization and International Trade
- Restrictions on free flow of data
- Limitations on use of aggregated data ("big data")
International Principles

A number of international instruments have been adopted in an effort

- To harmonize national and regional approaches
- To preserve fundamental privacy
- To prevent harmful restrictions on trade and development
Principles (1)

- **Collection Limitation Principle**: Personal data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

- **Data Quality Principle**: Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

- **Purpose Specification Principle**: The purposes for which personal data is collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
Principles (2)

- **Use Limitation Principle**: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified except with the consent of the data subject or by the authority of law.

- **Security Safeguards Principle**: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

- **Accountability Principle**: Those who collect and process personal data should be accountable for complying with measures which give effect to the principles stated above. Data controllers remain accountable for personal data under their control without regard to the location of the data.
Consumer Protection

- National laws on consumer protection also apply to cross-border transactions (especially business-to-consumer) and have the potential to create conflicts in regulation.

- In consequence the international community has also begun to adopt general principles on consumer protection, intended to modernize and harmonize national laws and regulations.

- Most recently the UN Guidelines on Consumer Protection in January 2016, intended to protect both consumer privacy and the global free flow of information, among other goals.
Principles (I)

- **Fair and equitable treatment.** Businesses should deal fairly and honestly with consumers at all stages of their relationship ... and should avoid practices that harm consumers, particularly with respect to vulnerable and disadvantaged consumers;

- **Commercial behavior.** Businesses should not subject consumers to illegal, unethical, discriminatory or deceptive practices, such as abusive marketing tactics, abusive debt collection or other improper behavior that may pose unnecessary risks or harm consumers.

- **Disclosure and transparency.** Businesses should provide complete, accurate and not misleading information regarding the goods and services, terms, conditions, applicable fees and final costs to enable consumers to take informed decisions.
Principles (2)

- **Protection of privacy.** Businesses should protect consumers’ privacy through a combination of appropriate control, security, transparency and consent mechanisms relating to the collection and use of their personal data;

- **Consumer complaints and disputes.** Businesses should make available complaints-handling mechanisms that provide consumers with expeditious, fair, transparent, inexpensive, accessible, speedy and effective dispute resolution without unnecessary cost or burden.
Conclusions

- If your company is involved in cross-border (transnational) transactions with consumers, you need to be aware of the rules in force in the foreign countries where you transact business. The rules on privacy, data protection and consumer rights are not the same as ours.

- International principles on these issues are evolving and businesses need to be aware of, and participate in, the discussions.

- Technology is moving faster than the principles.

- Make privacy, data protection and consumer protection a priority, a key part of your corporate culture and business goals.
On the Regulatory Frontier: Developing Insights from Payment Transactions

Jason Korosec
• Group Head & Senior V.P. for Business Intelligence
  MasterCard Advisors

Mark Edwin Burge
• Associate Professor of Law
  Texas A&M University School of Law

David P. Stewart
• Professor from Practice
  Georgetown University Law Center