Big Data and Enforcement Agency Oversight in 2018

Joyce Yeager, Esq., CIPM, CIPP/US

Assistant Attorney General, Office of the Missouri Attorney General, Unit Leader, Privacy and Multistates
The statements and opinions offered are the personal opinions of Joyce Yeager and are neither those of the Office of the Missouri Attorney General nor those of General Koster.
Consumer Consent at Heart of $1.35M Verizon, FCC “Supercookie” Settlement

Verizon has agreed to notify consumers about its targeted advertising programs and gain their consent before sharing its tracking data with third parties, the FCC announced [March 7, 2016].

The news comes as part of a settlement resolving the FCC’s investigation into the carrier’s controversial “supercookie” tracking program, in which Verizon attached unique, undeletable identifiers to customers without their knowledge to gather information about their Internet browsing habits.

Mon, 03/07/2016, wirelessweek.com, by Diana Goovaerts, Associate Editor
FCC Proposes Stricter Privacy Rules for Internet Service Providers

You should be able to decide what data your broadband or wireless provider shares with marketers. Period.

FCC Chairman Tom Wheeler has proposed new regulations to protect broadband and wireless customers' private data.

That's the message the Federal Communications Commission is sending with a proposed regulation intended to safeguard private customer information and to require broadband and wireless companies to get consumers' permission before sharing data with third parties such as marketers.

Chairman Tom Wheeler circulated his proposal among the other four FCC commissioners on [March 10, 2016]... Actual rules would likely be voted on later this year after the comment period ends.

by Marguerite Reardon, cnet, March 10, 2016
NHTSA is conducting a comprehensive review of the National Automotive Sampling System (NASS) research design and data collection methods as part of a major effort to modernize the system. Users of NASS and crash data may comment on the future utility of current data elements, recommend additional data elements and attributes, and describe their anticipated data needs.

FBI, NHTSA issue warning on vehicle hacks

Unauthorized access of standard systems -- or of after-market add-on systems -- might have many purposes, the agencies warned. . . .

And "while not all hacking incidents may result in a risk to safety -- such as an attacker taking control of a vehicle -- it is important that consumers take appropriate steps to minimize risk."

Mark Rockwell, FCW Magazine, March 18, 2016.
Securities and Exchange Commission

Jury Convicts in Big Data Insider Trading Trial

The US Securities and Exchange Commission won a jury verdict in a ‘big data’ insider trading case involving proprietary credit card transaction data. The defendants, who worked as data analysts for Capital One Financial Corp, made $2.8 million on a $147,300 investment, a return of about 1,800 percent, according to the SEC complaint.

Jury verdict
A federal jury in Philadelphia agreed with the SEC that the credit card information used by defendant Nan Huang to trade in shares of consumer retail companies ahead of earnings reports was “material.” The other defendant, Bonan Huang, settled with the SEC last month, agreeing to more than $4.7 million in penalties and other payments without admitting or denying the allegations.

Both defendants, who are not related, are Chinese nationals and fled to China after Capital One fired them last year, where they remain.

Profitable big data
The SEC accused the Huangs of making searches on Capital One’s proprietary database of credit card transactions relating to least 170 publicly traded companies from November 2013 to January 2015. The defendants used put or call options to trade retail stocks immediately before earnings releases.

By Sanford Bragg, January 20, 2016, integrety-research.com
National Association of Insurance Commissioners

NAIC to Explore Insurers’ Use of Big Data in 2016

Big data - the conversion of customer information collected and stored electronically into useful information - is changing how many insurers do business. While the use of big data can aid insurers’ underwriting, rating, and claim settlement practices, consumers’ rights to privacy and protection must be balanced.

On December 17, 2015, the National Association of Insurance Commissioners (NAIC) adopted the following charge:

• Explore potential opportunities for regulatory use of big data to improve efficiency and effectiveness of market regulation. If appropriate, make recommendations no later than the Fall National Meeting 2016 for 2017 charges for the D Committee to address any recommendations identified by the 2016 exploration.

• Specifically, the NAIC Market Regulation (D) Committee is reviewing the use of big data in property and casualty claims settlements and the Consumer Liaison Committee will review the use of big data in P&C price optimization rating methods. Additionally, the Life Actuarial Task Force (LATF) will examine the emerging trend of accelerated underwriting based on the use of big data.

by Sheila Coolidge, Senior Insurance Compliance Analyst, Wolters Kluwer Financial Services
February 15, 2016
STATE INSURANCE REGULATORS TAKING INITIATIVE ON CYBERSECURITY ISSUES

- The NAIC's Cybersecurity Task Force released a **Consumer Cybersecurity Bill of Rights** draft. The bill of rights is intended to set standards for helping consumers if their personal information is compromised. The Task Force expects to adopt these standards within the next 30 days.

- The Cybersecurity Task Force is also coordinating with state insurance regulators to **conduct examinations of insurance companies to verify companies are taking appropriate steps to protect sensitive data**, including confidential personal information.
March 17, 2016

Improper disclosure of research participants’ protected health information results in $3.9 million HIPAA settlement

Feinstein Institute for Medical Research agreed to pay the U.S. Department of Health and Human Services, Office for Civil Rights (OCR) $3.9 million to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules and will undertake a substantial corrective action plan to bring its operations into compliance. This case demonstrates OCR’s commitment to promoting the privacy and security protections so critical to build and maintain trust in health research. Feinstein is a biomedical research institute that is organized as a New York not-for-profit corporation and is sponsored by Northwell Health, Inc., formerly known as North Shore Long Island Jewish Health System, a large health system headquartered in Manhasset, New York that is comprised of twenty one hospitals and over 450 patient facilities and physician practices.
Institutional Review Boards/HHS

Research activities funded by the U.S. Federal Government must be supervised by an Institutional Review Board (IRB) or its equivalent, and many institutions conducting research with human subjects that are not federally funded follow the same procedures. IRBs are regulated by the U.S. Office of Health and Human Services. . . Researchers supervised by IRBs must respect participants’ privacy, secure informed consent, and maintain confidentiality. These ethical principles have practical consequences for research. They limit the ways that researchers may recruit participants... Whether the deidentified data of this sort can be shared with researchers outside the original IRB-approved team that collected it depends on several factors... Many big datasets in developmental science have restrictions on access either because the data were collected under Federal regulations that prohibit releasing individually identifiable data or because the participants were not asked for permission to share data with other researchers...

Rick O. Gilmore, onlinelibrary.wiley.com, January 24, 2016
U.S. Department of Agriculture

GOVERNMENT IMPETUS AND GATEKEEPER

• Smart farming and access issues for small and rural farmers to cellular and internet based information

• Smart farming and big ag sponsorship

• Seed design, soil usage, fuel usage

GOVERNMENT AS ENFORCER

The U.S. Department of Agriculture puts advanced analytics to work to root out fraud in the food stamp program, thereby using tax dollars more effectively. Beginning in the 1990s, when the agency migrated to benefits cards, it has used some form of analytics to detect suspicious patterns and hone in on those abusing the program. However, the agency's Supplemental Nutrition Assistance Program (SNAP) has recently stepped up efforts to root out abusers by focusing on stores and individuals engaged in trafficking Electronic Benefit Transfer (EBT) cards and skimming cash.
[CFPB Fined Dwolla $100,000] in First Data Security Enforcement Action

The Consumer Financial Protection Bureau (“CFPB”) gave the fintech online payment sector a “wake up call” with an enforcement action against a Des Moines start up digital payment provider, Dwolla, Inc. (“Dwolla”).

The CFPB alleged that Dwolla misrepresented how it was protecting consumers’ data. Dwolla entered into a Consent Order to settle the CFPB charges and agreed to pay a $100,000 penalty and to change and improve its current security practices. The CFPB never alleged that Dwolla had breached any consumer data. According to the CFPB, Dwolla “failed to employ reasonable and appropriate measures to protect data obtained from consumers from unauthorized access,” while telling consumers that the information was “securely encrypted and stored.” Dwolla, had over 650,000 customer accounts and was transferring as much as $5M a day in 2015.

Tuesday, March 8, 2016, The National Law Review, Christopher E. Hoyme
H. R. 4516

To require data brokers to establish procedures to ensure the accuracy of collected personal information, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES
FEBRUARY 10, 2016

Mr. JOHNSON of Georgia . . . introduced the . . . bill; which was referred to the Committee on Energy and Commerce
State Legislators as Regulators

With more schools and states contracting with online education companies, [state] legislators saw a need to lay out practices and procedures for these contracts, particularly with the news that Google mined student email for advertising purposes until earlier this year. [New] state laws spell out what those third-party contracts need to include, established procedures for security breach notification and data deletion, and prohibited companies from advertising to and selling data from students.

A National Look at Student Data Privacy Legislation by Tanya Roscorla, Government Technology, September 12, 2014
# The States as Regulators

<table>
<thead>
<tr>
<th>State Laws</th>
<th>.... Note the variety</th>
</tr>
</thead>
<tbody>
<tr>
<td>Arrest and Conviction Records</td>
<td>Legal filings</td>
</tr>
<tr>
<td>Banks and Financial Records</td>
<td>Mailing lists</td>
</tr>
<tr>
<td>Cable Television</td>
<td>Medical Records/Biological information/Bioidentifiers</td>
</tr>
<tr>
<td>Computer crime</td>
<td>Pharmacy Records</td>
</tr>
<tr>
<td>Credit Reporting and Investigating</td>
<td>Polygraphs in Employment</td>
</tr>
<tr>
<td>Criminal Justice Records</td>
<td>Privacy Statutes (such as the protection of certain pictures)</td>
</tr>
<tr>
<td>Education Records</td>
<td>Social Security numbers</td>
</tr>
<tr>
<td>Electronic Surveillance</td>
<td>State Constitutional guarantees</td>
</tr>
<tr>
<td>Employment Records</td>
<td>Sunshine Statutes</td>
</tr>
<tr>
<td>Government Information on Persons</td>
<td>Tax Records</td>
</tr>
<tr>
<td>Identity Theft</td>
<td>Telephone Services</td>
</tr>
<tr>
<td>Insurance Records</td>
<td>Testing in employment</td>
</tr>
<tr>
<td>Library Records</td>
<td>Tracking</td>
</tr>
<tr>
<td>Licensing Information</td>
<td>Vehicle/Drivers Licenses</td>
</tr>
</tbody>
</table>
Government, Big Data Purveyors

Open Records Statutes
In *United States v. Maynard*, the D.C. Circuit introduced a different approach, which could be called a "mosaic theory" of the Fourth Amendment. Under the mosaic theory, searches can be analyzed as a collective sequence of steps rather than as individual steps. Identifying Fourth Amendment searches requires analyzing police actions over time as a collective "mosaic" of surveillance; the mosaic can count as a collective Fourth Amendment search even though the individual steps taken in isolation do not. The D.C. Circuit applied that test in *Maynard* to GPS surveillance of a car. The court held that GPS surveillance of a car's location over twenty-eight days aggregates into so much surveillance that the collective sequence triggers Fourth Amendment protection.

When the Supreme Court reviewed *Maynard* in *United States v. Jones*, concurring opinions signed or joined by five of the justices endorsed some form of the D.C. Circuit's mosaic theory. The majority opinion resolved the case without reaching the mosaic theory, and neither concurring opinion gave the issue extensive analysis. But Justice Alito's concurring opinion for four justices clearly echoed the basic reasoning of the D.C. Circuit in concluding that long-term GPS monitoring of a car counts as a search even though short-term monitoring does not. Justice Sotomayor's separate concurrence also voiced support for the mosaic approach.
Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation. Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one’s not visiting any of these places over the course of a month. The sequence of a person’s movements can reveal still more; a single trip to a gynecologist’s office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story.

A person who knows all of another’s travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups — and not just one such fact about a person, but all such facts.
Courts as Regulators

In re Adobe Systems, Inc. Privacy Litigation
(2014) Judge Koh

Costs to mitigate risk of harm (future harm) are fairly traceable to lack of adequate security.

Note analysis of statutes by state and petition/complaint by count

In re Sony Gaming Networks...
(2014) Judge Battaglia

Representations about security are actionable as misrepresentations.

As to Missouri, the Court held that omissions or misstatements about security can be actionable if inducing a purchase.

Omissions can be actionable as unfair practice if consumers are misled.

FTC v. Wyndham Worldwide Corp.
(2015) Third Circuit

Third Circuit found that inadequate security can be the basis of an unfair practice claim under Section 5 (42 U.S.C. Section 45(a)).

The Court rejected Wyndam’s argument that it was entitled to know with ascertainable certainty of the FTC’s interpretation of what cybersecurity practices are required in order to comply with Section 45(a).
Plaintiffs’ Bar as Regulators

Shutterfly Biometric Data Privacy Class Action Moves Forward

On Dec. 29, [2015,] a federal judge in Illinois... denied Shutterfly’s motion to dismiss a potential class action lawsuit against the online photo publisher and subsidiary ThisLife LLC.

The class action lawsuit claims that Shutterfly... violated Illinois’ Biometric Information Privacy Act (BIPA) through their use of facial recognition technology.

In their motion to dismiss..., Shutterfly and ThisLife stated that face geometry scans derived from photograph images and not an actual person were not covered under the Illinois BIPA.

Shutterfly argued that the Act had specifically excluded photographs and that BIPA was enacted to protect a person’s financial information. The company argued that their tagging system only includes arbitrary tags without a link to any individual’s personal or financial information....

Notably, Illinois law also prohibits companies that collect biometric data from selling it to third parties.

January 5, 2016, Injury Attorney at Your Service
“First, the FTC is an enforcement agency and it can and should use its traditional deception and unfairness authority to stop consumer harms that may arise from the use of Big Data.” Commissioner Ohlhausen, August 5, 2014.

THE FTC AND THE NEW COMMON LAW OF PRIVACY, Daniel J. Solove and Woodrow Hartzog, 114 Columbia Law Review, 583 (2014). “FTC’s privacy jurisprudence is functionally equivalent to a body of common law... The FTC has codified certain norms and best practices and has developed some baseline privacy protections.”

FTC Casebook, International Association of Privacy Professionals
Privacy and Data Security Enforcement Actions
https://iapp.org/resources/ftc-casebook

“[J]ust as Big Data can be used to extend credit, educational opportunity, and health benefits to consumers, so too can it be used to deny those services.” Director Jessica Rich, May 11, 2015.
Fairness - Section 5 of the FTC Act

Quoting Solove and Hartzog:

The primary source of authority for FTC privacy enforcement was Section 5 of the FTC Act, which prohibits “unfair or deceptive acts or practices in or affecting commerce.” An “unfair or deceptive” act or practice is a “material representation, omission or practice that is likely to mislead a consumer acting reasonably in the circumstances, to the consumer’s detriment” or a practice that “causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.” Thus, in its enforcement under Section 5 of the FTC Act, the FTC had two bases for finding privacy violations – “deceptive” trade practices and “unfair” trade practices.
Unfairness - the FTC Act and Mini-FTC Acts

Missouri Statute

The [Missouri Merchandising Practices Act] was enacted “to preserve fundamental honesty, fair play, and right dealings in public transactions,” . . . and prohibits “deception, fraud, false pretense, false promise, misrepresentation, unfair practice or concealment, suppression, or omission of any material fact in connection with the sale or advertisement of any merchandise in trade or commerce.” Mo. Rev. Stat. § 407.020(1). To state a claim under the MMPA, a plaintiff must allege: (1) the purchase of merchandise; (2) for personal, family, or household purposes; and (3) an ascertainable loss of money or property as a result of an act or practice declared unlawful under the MMPA.
Unfairness and the FTC Act and Mini-FTC Acts

“All states have enacted unfair and deceptive trade practices statutes (known as ‘Little FTC Acts’) modeled, at least in part, on the federal law... The “unfair practices” definition promulgated by the [Missouri Attorney General] in [regulation] 15 CSR 60–8.020 closely resembles the early policy statement of the FTC as to its definition of unfairness.

“[Section 60-8-020] defines an unfair practice as ‘any practice which: (A) Either—1. Offends any public policy as it has been established by the Constitution, statutes or common law of this state, or by the Federal Trade Commission, or its interpretive decisions; or 2. Is unethical, oppressive or unscrupulous; and (B) Presents a risk of, or causes, substantial injury to consumers.’”
State Attorneys General

Privacy Enforcement Pioneers: The Role of Attorneys General in the Development of Privacy Law

Danielle Keats Citron
February 16, 2016
Notre Dame Law Review, Forthcoming

• Multistate Efforts
  – TJX
  – Google Street View cars

• AGs also enforce provisions of GLBA and other statutes with privacy protections for individuals
16. Respondent, its owners, members, and officers agree to comply with the requirements of Section 407.1500 (breach notification statute), and shall maintain adequate data security measures, including but not limited to:

a. Respondent shall maintain and follow all reasonable policies and procedures necessary to ensure the protection of personal health information;

b. **Respondent shall seek proper authority, as provided by contractual agreement with the owners of data, to create and implement programing changes which may affect the safety and security of personal health information**;

c. Respondent shall follow policies and procedures for data security testing *in compliance with the terms of any contract* between Respondent and the Missouri Department of Social Services;

d. Respondent shall make all commercially reasonable efforts to minimize data vulnerabilities;

e. Respondent shall train employees in proper data security and applicable policies and procedures; and

f. Respondent shall **not improperly and knowingly disclose personal health information to a third party.**
The People as Regulators

AMENDING CONSTITUTION
BY BALLOT

Missouri Constitution
Article I   BILL OF RIGHTS   Section 15

Unreasonable search and seizure prohibited--contents and basis of warrants.

Section 15. That the people shall be secure in their persons, papers, homes, effects, and electronic communications and data, from unreasonable searches and seizures; and no warrant to search any place, or seize any person or thing or access electronic data or communication, shall issue without describing the place to be searched, or the person or thing to be seized, or the data or communication to be accessed, as nearly as may be; nor without probable cause, supported by written oath or affirmation.

Source: Const. of 1875, Art. II, § 11. (Amended August , 2014)

PATIENT FEARS IMPACT
HEALTH CARE

HIPAA Breaches: Minimizing Risks and Patient Fears
IndustryView | 2015
Software Advice

Nearly one-quarter of patients (21 percent) withhold personal health information from their doctors due to data security concerns.

A majority of patients (54 percent) are “moderately” or “very likely” to change doctors as a result of a patient data breach.
The statements and opinions offered are the personal opinions of Joyce Yeager and are neither those of the Office of the Missouri Attorney General nor those of General Koster.
Compliance and regulatory oversight
Does ethical theory offer a framework?

TELEOLOGICAL - This describes an ethical theory which judges the rightness of an action in terms of an external goal or purpose. So, according to a teleological theory, consequences always play some part, be it small or large, in the determination of what one should or should not do. Yeager Note: Are we about consequences in light of potential enforcement actions? If so, such an approach can fail to account for enforcement from an unexpected source or the expense from potential action in enforcement.

CONSEQUENTIALIST - Under a consequentialist theory, the consequences of an action determine its moral value. A key question in consequentialist theory is how to measure the moral worth of the consequences. Consequences can be good, neutral, or evil. Another relevant question is which consequences count (intended or actual). If only actual consequences count, then do all consequences count? Yeager Note: Are we about consequences in light of potential enforcement actions? If so, such an approach can fail to account for enforcement from an unexpected source or the expense from potential action in enforcement.

RELATIVISM/SUBJECTIVISM - This type of theory denies that there is any uniquely right moral theory, standard, or value. Everything is subjective. For example, Jean Paul Sartre claimed that each individual creates his or her own morality based solely on one's own decisions about what is valuable. There are no moral standards to turn to that have any more authority than those that you create. Things (including other people) only have value because you gave them value. Yeager Note: Absent adequate controls, institutions with such an outlook may have difficulty responding to questions posed by enforcers or consumers, I offer.

DEONTOLOGICAL - This type of theory claims that there are features within the actions themselves which determine whether or not they are right. These features define the extent to which the actions conform with recognized moral duties. Deontological theories do not consider consequences to be important when determining whether or not an action is ethical. It doesn’t matter if the drunk driver made it home safely. Yeager Note: Does this viewpoint allow for each participant in the life cycle to look at the Fair Information Practices Principles as a standard for normative behavior? Note that this also may allow for operation of virtue based ethical theories. I would also argue this is the viewpoint most capable of adapting to change in technologies and attitudes.