Coalition Against Insurance Fraud

JOURNAL OF INSURANCE FRAUD IN AMERICA

Can insurers fight fraud while privacy vanishes?

Fraud fighters must guard privacy rights yet meet crime-fighting needs

by MATTHEW SMITH, ESQ.| May 31, 2017

A billionaire tossed a verbal stone into an electronic pond, causing ripples worldwide.“ All these concerns about privacy tend to be old-people issue,” [1] LinkedIn founder Reid Hoffman proclaimed about the new world of electronic communication.

However Hoffman defines “old people,” today’s electronic communication-linked world is raising privacy concerns across all generations. From retail breaches such as Target Corporation, through the credit-card account fiasco engulfing Wells Fargo, privacy invasions and protection are key topics.

Fraud investigations are a big part of the privacy conversation. Many tools used by investigators today were only Star Wars technology a generation ago. Predictive modeling, tracking cell conversations and the ever-expanding world of social-media probes all help battle insurance fraud. Some consumer groups and trial attorneys representing insureds express concern about how insurers use technology to redefine the relationship between insured and insurer. Many concerns have merit because the relationship between insurance carrier and policyholder derives from a written policy contract.

Insurers routinely invoke policy language. They cite the “duty to cooperate” or “duties in the event of loss.” Yet most policy language was written before cell phones and social media. Insurers are woefully deficient in updating policies to keep pace with rapidly changing electronic communication and a data-driven society.

Insurers and related organizations finally are addressing how privacy, claim investigations and policy contracts must be adapted for this new era. How well it is done will define how emerging technology is used in fraud investigations for future generations.

Fraud fighters must set standards so data and technology are properly used and guard personal privacy rights. Otherwise, courts and legislatures will impose those standards. That could have a profound impact — positive or negative — on the fraud fight.

Privacy issues facing fraud investigators today stretch far beyond social media. While *Facebook, Twitter, Instagram* and other platforms create a treasure trove of information for fraud investigations, the future bodes an entire new realm of data unlike any we have known. Welcome to the world of "big data."

Big data involves data sets that go beyond the ability of commonly used software to capture, analyze and process. [2]

The world's technological *per-capita* capacity to store information has doubled every 40 months since the 1980s, and has grown exponentially since 2012. [3] Big data today is measured in zettabytes. That is one sextillion bytes of information — a "1" followed by 21 zeroes. The entire World Wide Web contained half of one zettabyte of data in 2009. [4]

Billions of devices leave clues

Data collection no longer derives from human interactions. The Internet of Things (IoT) is an ever-growing worldwide network of non-human physical objects that feature an IP address for internet connectivity. They can communicate information without human

assistance. Many trace the birth of IoT to 1982 when a Coke machine was modified at Carnegie Mellon University. The machine reported its inventory and temperature to a remote location. [5]

Today the IoT collects data from items as simple as toasters, home thermostats, and washers and dryers to entire electrical grids and transportation systems for the world's largest cities. IoT devices will top 50 billion by no later than 2020. [6] These devices collect, share and retain data without human interaction.

For insurance-fraud investigations, the Internet of Things moves from a worldwide data cloud to retrieving valuable information: black box data concerning vehicle speed, braking and other information relevant to how an auto accident occurred to security panel downloads identifying who entered a building, and at what time before a major fire loss happened. How this data is authorized to be collected, what type of analysis is needed to ensure accuracy, and whether and how it is admissible in court are all issues that involve fraud investigators today.

"For insurance-fraud investigations, the Internet of Things moves from a worldwide data cloud to retrieving valuable information …"

Each of these these billions of devices leaves a data trail while communicating with each other throughout the world. Linking these electronic bits of evidence allows this information to be captured,

analyzed and sold for its analytical value. Big-data analytics alone are valued at more than $100 billion and its growth rate exceeds10 percent a year. That is more than double the pace of “traditional” software business analysis. [7]

How does big data help investigate insurance fraud? A telling case comes from Middletown, Ohio.

A fire broke out in Ross Compton’s home on Sept. 19, 2016. Compton frantically called 911. He reported the fire. He claimed he packed a few belongings in a suitcase, grabbed his computer, used his cane to break out a window, and hurled items out of the house before rushing out to save himself.

Investigators determined the fire was intentionally set. They subpoenaed the data from Compton’s pacemaker and heart monitor. A cardiologist showed Compton allegedly was not doing the strenuous physical activity he claimed during the 911 call. He was indicted for arson.

Insurance investigators use data analytics for purposes ranging from predictive models of workers-compensation injury red flags to vehicle license-plate reader reports purchased from databases containing billions of “hits” tracking vehicles as they move through public highways, parking lots and garages.

How data is being secured equally involves a number of options.They range from court-ordered subpoenas to companies providing access to databases and personal information with programs built for predictive modeling or claim investigations.

While the universe of data changes constantly, unchanged are authorization forms and out-of-date insurance-policy language. Virtually no policy contains provisions relating to compiling, using or analyzing personal data or big data for investigating fraud. This leaves a wide gap for attorneys and consumer advocates to assert insurers already are going too far

U.S. lags in privacy laws

Many Americans believe a right of privacy is enshrined in the Constitution. Privacy actually traces back to 1890. Samuel D. Warren and Louis D. Brandeis published "*The Right to Privacy*." They advocated for a general common-law privacy protection. No U.S. court recognized such a right at the time.

Brandeis was a Supreme Court Justice when he authored the majority opinion in *Olmstead vs. United States*. [8] The court laid out a constitutional right "to be let alone." Now every jurisdiction in the U.S. recognizes some form of a constitutional, common law or statutory right of privacy.

That right, however, has limits. Hoffman's quote about privacy being for "old people" partially derives from the willingness of Millennials to give up more personal data than any generation before. In exchange, they gain the ability to readily access online information. Thus there is equally the right to surrender private data and information for some benefit or information.

A privacy right also may be surrendered by contractual agreement. This is where many insurers find themselves today, either through claims authorizations or using broad, archaic policy language to incorporate electronic data access.

The U.S. Congress and virtually all 50 state legislatures are considering updated privacy legislation. The U.S. lags behind many nations in establishing privacy laws. More than 80 countries have adopted comprehensive data protection laws. The U.S. remains notable for this gap. [9]

Canada adopted the Personal Information Protection and Electronic Documents Act in 2001. Privacy protections for data processing in Europe were concluded within the Council of Europe in 1981. European citizens' rights to data privacy also are protected under the European Convention on Human Rights. It protects an individual's "private and family life, home and correspondence."

The closest U.S. national protection is the Gramm-Leach-Bliley Act. Corporations, including insurers, must provide customers a written "privacy notice" advising how personal data and information are used. Supporters of the legislation could not foresee the dramatic rise of "big data" the new millennium would bring.

"Insurers must do a better job of including language regarding insurance fraud …"

Insurers annually provide policyholders a federally compliant privacy statement. Many insurer fraud fighters, however, have no input into their company's privacy language.

Often these statements contain lukewarm language such as: "*We will not use your personal data for any purpose other than underwriting and setting of a fair premium.*" Attorneys in a lawsuit thus can assert impropriety when personal data is used to investigate claims. Insurers must do a better job of including language regarding insurance fraud in the permitted scope of private information and data collection.

Insurers should work cooperatively with groups such as the Coalition Against Insurance Fraud and National Insurance Crime Bureau on legislation impacting use of private data.

These organizations help draft legislation, and lobby statehouses, to ensure legislation is fair and equitable to all parties. The Coalition and

NICB also monitor court cases affecting fraud investigations, including privacy issues. Both organizations file *amicus curiae* briefs with state and federal courts, seeking fair application of the law in combating fraud. The Coalition is uniquely positioned to be a strong — and balanced — privacy advocate with its insurer and consumer members.

Legislation and court decisions ahead will dramatically define the scope of what personal data may be used, and how, in all aspects of our society — including insurance fraud.

Facebook clues discoverable

Key criminal cases offer a guide for the future of insurance fraud investigation.

The New York Court of Appeals issued a decision involving *Facebook* on April 4, 2017. [10] The New York County DA issued 381 warrants seeking access to user account information involving a criminal investigation of alleged Social Security disability fraud. *Facebook* moved to quash the warrants. It argued the warrants were constitutionally defective, over-broad and that *Facebook's* users were entitled to personal privacy protection. The trial court directed *Facebook* to immediately comply with the warrants.

Facebook appealed. The New York high court upheld the warrants. Recognizing today's world of electronic data, the court noted a

traditional search warrant authorizes law enforcement to enter, search and seize property.

“The trial court directed Facebook to immediately comply with the warrants.”

“These differences in execution, however, can be easily explained by the nature of the materials sought. The service provider is more likely to be better equipped to access and conduct a search of its own digital information than law enforcement personnel, and the data may be stored in different locations,” the court noted. [11]

Arkansas saw a dispute arising from a search warrant issued by the Bentonville Police Department to Amazon.com. The defendant James Andrew Bates allegedly murdered Victor Collins, whose body was found at Mr. Bates’ residence.

Crime investigators noted an Amazon Echo device in his home. The Amazon Echo or “Alexa” device is wireless equipment containing seven microphones equipped with sensors that use beam-forming technology to hear users from any direction.

Alexa can analyze speech, answer questions or respond to directives — including to other internet-connected devices. Bates also owned numerous Wi-Fi connected devices, including a “Nest” thermostat, home alarm system with door-monitoring alarms and motion sensors,

weather monitor and remote-control lighting. Collectively, these devices can be remote controlled by cellphone, computer or similar devices. The court approved a search warrant directing Amazon to provide access to all information Alexa recorded during the time surrounding the murder.

As more homes become digitally equipped, more requests for stored data will arise for fraud investigations. The *Facebook* decision confirms that courts will allow securing such data when appropriate steps are taken to secure release of information.

Insurers seeking the same data may not enjoy the same privileges as law enforcement. Instead, they must rely upon updated policy language and re-drafted authorization forms to conform with today's world of technology. Unless insurers do so, very relevant documents may not be discoverable.

Must ensure data admissible

Big data, the Internet of Things and the new world of communication information are breakthroughs in the fraud fight. We have at our fingertips today more information than anyone would have imagined a generation ago. At risk is whether insurers are moving promptly enough, and in the right direction, to ensure data and information are obtainable and admissible in court.

In addition to updating policy language and forms, insurers and consumer advocacy groups must work together to develop best practices for collection and use of this data.

Historically, insurers often moved in an authoritative, corporate manner. Courts thus found insurance policies to be unfairly one-sided "contracts of adhesion." Insurers today face a unique opportunity to work cooperatively to adopt fair and equitable best practices and write new policy language that allows reasonable collection and use of data for underwriting, premium determination, claims and fraud investigation.

Insurers and consumers should develop mutually acceptable standards and practices as the world of big data evolves, rather than face a patchwork of 50 or more differing rules, regulations and laws.

Whether those standards are developed as a model act for state legislation or through appropriate channels as accepted industry standards also needs deciding.

Insurers can work cooperatively with consumer-advocacy groups and legislatures in a forward-thinking manner. Or they can simply wait and "see what happens." Yet doing nothing is not an option. Decisions today will guide how this valuable treasure trove of information is used, or lost, for generations of insurance fraud investigators to come.

About the author: Matthew J. Smith, Esq. is associate director of government affairs for the Coalition Against Insurance Fraud, and Of Counsel to the law firm of Smith, Rolfes and Skavdahl, Co., LPA, which he founded in 1989. Mr. Smith is a frequent lecturer on insurance law matters across the U.S.