PROPERTY CASUALTY360°

September 18, 2017

The death of privacy

Here's how big data is opening up a world of discoverable information

By: Dennis Jay

Ross Compton woke up one morning to find his house on fire. The Ohio man tossed a large load of possessions outside, then climbed out of his bedroom window as the flames engulfed his home.

Or so he said.

Creative investigators subpoenaed data from his pacemaker. Someone in Compton's condition couldn't possibly have clambered around the way he claimed, the downloaded data allegedly shows. Prosecutors say he torched the house for the insurance money.

Compton's pacemaker case is churning national headlines. His unusual case rings privacy bells that could deeply affect the fraud fight, for better or worse.

America is a giant black box, morphed by the emergent Internet of Things (IoT) and big data. Growing motherlodes of personal consumer data are being generated by a digitally hyper-connected society. Endless zettabytes of granular information are being stockpiled about our activities, thoughts and intentions throughout each day.

Some 50 billion IoT devices will silently connect, sift and store information about people's daily lives by 2020.

Fraud investigators are gaining new superpowers from these data gushers. Courts widely find much of this personal data is discoverable for insurance-fraud cases. Judges regularly overrule the defense's privacy objections if investigators follow proper procedures for legally obtaining data. Still, vigorous privacy debates are at work in America and privacy is far from dead.

Law enforcement can routinely invoke subpoenas to obtain personal data in criminal cases. Insurer subpoena access is derived solely from policy conditions generally triggered by an insured's bad-faith civil action after the insurer denies a claim for suspected fraud. Much is at stake in these costly suits.

Yet most insurance policy contracts and privacy notices are outdated. They were written decades ago during a time of typewriters and manila folders. The archaic wording doesn't reflect today's ever-expanding data and advancing technology. Nor does it clearly outline anti-fraud obligations in a digital era. Increasingly, insurers risk having data searches in civil fraud actions and investigations declared undiscoverable as privacy violations.

> ***Simply "doing what we've always done" isn't an option. We have an unparalleled opportunity to help lead privacy into a modern, data-rich era that benefits the fraud fight and consumers alike.***
>
> Coalition Against Insurance Fraud

Insurers have the opportunity to modernize their privacy best practices, and policy contract and privacy language. The language should clearly address insurance fraud in the permitted scope of private information and data collection.

It's a careful balance to preserve insurer rights to root out costly fraud schemes while protecting people's legitimate privacy rights. Insurers can become more widely viewed as responsible corporate citizens who are helping to shape the privacy discussions for the benefit of all concerned.

Unless insurers take that lead, others may impose over-reaching privacy laws, regulations and court rulings. The results could stifle fair and reasonable access to actionable data.

Data sources expanding

New forms of digital evidence are continually being developed by our data-rich society, delving deeper into people's lives and creating questions about privacy limits. Courts generally uphold this kind of data discovery in criminal fraud cases, so far, as seen in these cases:

Social-media postings are generally accessible to fraud investigators — even behind privacy settings.

Ross Compton challenged his pacemaker search as a privacy violation. The judge allowed the data collection, calling the probe of his heartbeats, “no big deal.”

Recent Fitbit searches have also held up so far.

Richard Dabate says he found his wife, Connie, dead and zip-tied to a chair in their Hartford, Connecticut-area home. Dabate said an intruder shot her, but Connie's Fitbit allegedly recorded her moving around nearly an hour after the time Dabate said she had been killed. Prosecutors say he tried to cash in Connie's $475,000 life insurance policy just five days after she died. Dabate is charged with her murder.

More data sources likely will keep emerging, such as:

Telematics. Sensors packed into vehicles could open up a wider world of vehicle data before long. Was the driver's parked SUV banged up by a hit-and-run driver two days after the owner bought auto coverage; or did the accident happen three days before, when he was uninsured?

Wearables. Work vests and other clothing embedded with sensors can help employers track an employee's whereabouts and activities throughout each day. Did that claimed injury happen at the loading dock when sensors suggest he was sitting quietly at a desk?

Home appliances. Home appliances and other non-traditional devices could be fair game as they load up with internet-connected sensors.

A homeowner's coffee pot brewed java in his kitchen, even though he said he was visiting friends across town when his house caught fire.

Will a garage door reveal a dishonest claimant's SUV location and movements? Will the interactive screen on the refrigerator door detail a busy grocery trip by a workers-comp claimant who insists she's immobilized by a painful back injury?

Digital assistants. Victor Collins was found dead in the backyard hot tub of James Andrew Bates in Bentonville, Ark. Bates called it an accident. Investigators suspect Bates drowned Collins, so they subpoenaed data from Bates’ obedient Amazon Echo digital assistant, “Alexa.” Bates disclosed the data despite privacy and First Amendment objections from Amazon in court. This is a murder case, yet it speaks to the potential for data-mining digital assistants in fraud investigations.

Update privacy efforts

Valuable fraud evidence could be successfully challenged by defense counsel in insurer lawsuits as improperly obtained. Outdated policy contracts and privacy notices may not hold up under privacy scrutiny.

Policies. Consumers voluntarily concede certain privacy rights via contract when they buy insurance policies. The policy contract defines an insured's duty to cooperate, and produce records and documents. Language such as “duty to cooperate” or “duties in the event of a loss” largely defines insurer contractual access to customer data. Yet virtually no policies define what that means. Nor do they reflect the storage and downloading of digital information from data-rich mobile devices, email, laptops, zip drives, the cloud and broader IoT.

Privacy notices. Federal law requires corporations to provide customers with an annual privacy notice advising how their personal information will be used. Yet insurer privacy statements frequently are very general. Like the policy language, most privacy notices were written well before the IoT and big data explosions, and rarely do they reference using information for fraud investigations.

Thus, the notices typically don't specify how the insurer will protect today's complex new personal data in a digitally hyper-connected society.

Take the privacy lead

Insurers can be proactive when it comes to protecting electronic data used in fraud investigations. Steps to take include:

Adopting best practices. Insurers should consider developing best practices and protocols for privacy. A written framework might cover compiling, storing and using personal data.

They could clarify insurer privacy practices across all lines and markets. SIU, claims, underwriting and sales are just some of the departments that must be closely involved in drafting these practices. Privacy protocols should be approved at the insurer's highest levels and special investigative units (SIUs) must be heavily involved.

Influencing legislation. The U.S. Congress and all 50 states are considering updated privacy legislation. Our nation lags behind most other nations in codified privacy protections, however, change is coming. Insurers and those who fight fraud are vulnerable unless they are part of the discussion.

Develop standards. The anti-fraud community can work cooperatively with consumer groups and other leaders to develop consensus on best privacy practices that preserve legitimate anti-fraud efforts, while acknowledging personal privacy rights.

Simply “doing what we’ve always done” isn't an option. We have an unparalleled opportunity to help lead privacy into a modern, data-rich era that benefits the fraud fight and consumers alike.