READ IT IN PRINT!
GET ONE YEAR (6 ISSUES) FOR JUST $14.95

- SUBSCRIBE TODAY!
- GIFT SUBSCRIPTION
- DIGITAL EDITION

Is Hacking the Future of Scholarship?

Once scholars begin—and the day is coming—hacking devices to find out more about influential people, the courts and the academic community will be faced with privacy decisions to make.

Share Tweet ShareThis

(PHOTO: ANDREY_POPOV/SHUTTERSTOCK)

September 27, 2013 • By Allen Porter Mendenhall • No Comments

Most attorneys are familiar with e-discovery, a method for obtaining computer and electronic information during litigation. E-discovery has been around a long time. It has grown more complex and controversial, however, with the rise of new technologies and the growing awareness that just about anything you do online or with your devices can be made available to the public. Emails, search histories, voicemails, instant messages, text messages, call history, music playlists, private Facebook conversations (not just wall posts)—if relevant to a lawsuit, these and other latent evidence, for better or worse, can be exposed, even if you think they've been hidden or discarded.

Anyone who has conducted or been involved with e-discovery realizes how much personal, privileged, and confidential information is stored on our devices. When you "delete" files and documents from your computer, they do not go away. They remain embedded in the hard drive; they may become difficult to find, but they're there. Odds are, someone can access them. Even encrypted files can be traced back to the very encryption keys that created them.

E-discovery has been used to uncover registries and cache data showing that murderers had been planning their crimes, spouses had been cheating, perverts had been downloading illegal images, and employees had been stealing or compromising sensitive company data or destroying intellectual property. Computer forensics were even used to reveal medical documents from Dr. Conrad Murray's computer during the so-called "Michael Jackson death

Search this website... Search

What is Energy East?
www.energyeastpipeline.com
Learn More About The Proposed Canadian Pipeline Project.

POPULAR LATEST
TODAY WEEK MONTH ALL

We Don't Know What to Eat

From the Mouths of Rapists: The Lyrics of Robin Thicke's 'Blurred Lines'

The Scientific Debate About GM Foods Is Over: They're Safe

Ireland Is Dying

Why Is Breakbone Fever Back in Florida?

Want Quick, Accurate Thinking? Ask a Musician

We Aren't the World

John McEnroe and the Sadness of Greatness

The Virtuous Circle of Ever-Lasting Expansion of Domestic Demand and

Web2PDF
converted by Web2PDFConvert.com

documents from Dr. Conrad Murray's computer during the so-called "Michael Jackson death trial."

More information is good; it helps us to understand our universe and the people in it. The tracking and amassing of computer and electronic data are inevitable; the extent and details of their operation, however, cannot yet be known.

Computer forensics can teach you a lot about a person: the websites he visits, the people he chats with, the rough drafts he abandons, the videos he watches, the advertisements he clicks, the magazines he reads, the news networks he prefers, the places he shops, the profiles he views, the songs he listens to, and so on. It is fair to say that given a laptop hard drive, a forensic expert could nearly piece together an individual's personality and perhaps come to know more about that person—secret fetishes, guilty pleasures, and criminal activities—than his friends and family do.

In light of this potential access to people's most private activities, one wonders how long it will be until academics turn to computer forensics for research purposes. This is already being done in scientific and technology fields, which is not surprising because the subject matter is the machine and not the human, but imagine what it would mean for the humanities? If Jefferson had used a computer, perhaps we would know the details of his relationship with Sally Hemings. If we could get ahold of Shakespeare's iPad, we could learn whether he wrote all those plays by himself. By analyzing da Vinci's browsing history, we might know which images he studied and which people he interacted with before and during his work on the Mona Lisa—and thus might discover her identity.

There are, of course, government safeguards in place to prevent the abuse of, and unauthorized access to, computer and electronic data: the Wiretap Act, the Pen Registers and Trap and Trace Devices Statute, and the Stored Wired and Electronic Communication Act come to mind. Not just anyone can access everything on another person's computer, at least not without some form of authorization. But what if researchers could obtain authorization to mine computer and electronic data for the personal and sensitive information of historical figures? What if computer forensics could be used in controlled settings and with the consent of the individual whose electronic data are being analyzed?

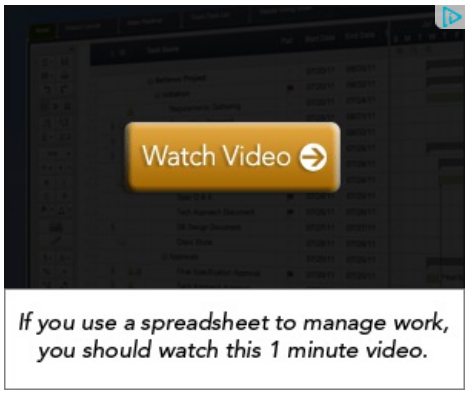
Consent, to me, is crucial: It is not controversial to turn up information on a person if he voluntarily authorized you to go snooping, never mind that you might turn up something he did not expect you to find. But under what circumstances could computer forensics be employed on a non-consensual basis? And what sort of integrity does computer or electronic information require and deserve? Is extracting data from a person's laptop akin to drilling through a precious fresco to search for lost paintings, to excavating tombs for evidence that might challenge the foundations of organized religion and modern civilization, or to exhuming the bodies of dead presidents? Surely not. But *why not*?

We have been combing through letters by our dead predecessors for some time. Even these, however, were meant for transmission and had, to that end, intended audiences. E-discovery, by contrast, provides access to things never meant to be received, let alone preserved or recorded. It is the tool that comes closest to revealing what an individual actually thinks, not just what he says he thinks, or for that matter, *how* and *why* he says he thinks it. Imagine retracing the Internet browsing history of President Obama, Billy Graham, Kenneth Branagh, Martha Nussbaum, Salmon Rushdie, Nancy Pelosi, Richard Dawkins, Toni Morrison, Ai Weiwei, or Harold Bloom. Imagine reading the private emails of Bruno Latour, Ron Paul, Pope Francis, Noam Chomsky, Lady Gaga, Roger Scruton, Paul Krugman, Justice Scalia, or Queen Elizabeth II. What would you find out about your favorite novelists, poets, musicians, politicians, theologians, academics, actors, pastors, judges, and playwrights if you could expose what they did when no one else was around, when no audience was anticipated, or when they believed that the details of their activity were limited to their person?

This is another reason why computer and electronic data mining is not like sifting through the notes and letters of a deceased person: having written the notes and letters, a person is aware of their content and can, before death, destroy or revise what might appear unseemly or counter to the legacy he wants to promote. Computer and electronic data, however, contain

Labor Supply Is Broken: Yes, Ireland Really Is Dying

Why Are Sold-Out Flights From South America Leaving Half Empty?



The Motivational Power of Media

Environmentalism? Perhaps. Environmentalists? Ewww!

Want Quick, Accurate Thinking? Ask a Musician

The Heightened Sensitivity of Romance Readers

Texting and the Stressed-Out Freshman

What Does Being a Vegetarian Say About You?

You Call That Aggressive? Not Compared to 'Grand Theft Auto'!

Online, Mozart in Background Boosts Women's Attractiveness

Porn Viewing Impacts Attitudes on Women in Workplace

Reality TV May Warp Viewers' Perception of Actual Reality

For Many, Playing the Lottery Undermines Self-Control

The Defensive Message in a Designer Handbag

Should We Bomb Syria? The Answer Is Easy if You Believe in Evil

Playing Prokofiev Is a Pain

The Enduring Appeal of Memory-Evoking Music

Web2PDF
converted by Web2PDFConvert.com

information that the person probably doesn't know exists.

More information is good; it helps us to understand our universe and the people in it. The tracking and amassing of computer and electronic data are inevitable; the extent and details of their operation, however, cannot yet be known. We should embrace—although we don't have to celebrate—the technologies that enable us to produce this wealth of knowledge previously unattainable to scholars, even if they mean, in the end, that our heroes, idols, and mentors are demystified, their flaws and prejudices and conceits brought to light.

The question is, when will we have crossed the line? How much snooping goes too far and breaches standards of decency and respect? It is one thing for a person to leave behind a will that says, in essence, "Here's my computer. Do what you want with it. Find anything you can and tell your narrative however you wish." It is quite another thing for a person never to consent to such a search and then to pass away and have his computer scanned for revealing or incriminating data.

It's hard to say what crosses the line because it's hard to know where the line should be drawn. As Justice Potter Stewart said of hard-core pornography, "I shall not today attempt further to define the kinds of material I understand to be embraced within that shorthand description; and perhaps I could never succeed in intelligibly doing so. But I know it when I see it." Once scholars begin—and the day is coming—hacking devices to find out more about influential people, the courts and the academic community will be faced with privacy decisions to make. We will have to ask if computer and electronic data are substantially similar to private correspondence such as letters, to balance the need for information with the desire for privacy, to define what information is "private" or "public," and to honor the requests of those savvy enough to anticipate the consequences of this coming age of research.

Amid this ambiguity, one thing will be certain: Soon we can all join with Princess Margaret in proclaiming, "I have as much privacy as a goldfish in a bowl." That is good and bad news.

Related Stories

College Guys Will Remember the Pretty Ones

UPDATE: Women Like Sex

What Does Being a Vegetarian Say About You?

Women as Literal Targets of Misogyny

Recommended by

13

Subscribe to Our Weekly Email Newsletter

Email Address

Subscribe

More like this: Education Tags: E-Discovery, Privacy, Security

About Allen Porter Mendenhall

Allen Mendenhall is a staff attorney to Chief Justice Roy S. Moore of the Supreme Court of Alabama, an adjunct professor at Faulkner University Thomas Goode Jones School of Law, and a doctoral candidate in English at Auburn University.

Time Tracking Free Trial
www.Replicon.com/Free_Trial
Easily Track Employee Time/Expense Used by 7,800 Companies, 1.5M Users

Life Insurance up to 85

How to Stop Your Divorce.

LexisNexis® Litigation

Disabled in Canada?

Sponsor a Girl Today

Simple Project Management

Web2PDF
converted by Web2PDFConvert.com

AROUND THE WEB

A Trick that Adds $1k to Social Security Checks Moneynews

Why You Should Stop Using Shampoo First To Know

Avoid Alzheimer's Disease: Here's What May Cause It
Newsmax Health

French Kissing: How to Do It the Right Way Lifescript

ALSO ON PACI

We Don't

Why Do W

Europe R

The Heig
2 comments

0 comments

Leave a message...

Best Community

No one has commented yet.

Subscribe Add Disqus to your site

COPYRIGHT © 2013 · PACIFIC STANDARD

Web2PDF
converted by Web2PDFConvert.com