Article

Prepared by: Caroline Shaffer Westerhof,
California National University for Advanced Studies

Nigeria: Protecting Financial Data from Cyber Attacks

EMMA OKONJI

Learning Outcomes

After reading this article, you will be able to:

- Understand why many cyber attacks come from China and Russia.
- Discuss the anti-cybercrime objectives of Palo Alto Networks.
- Describe what is meant by "application-shift," and how it presents a vulnerability.

Cyber attacks on organisations' data, be it financial or otherwise, are increasing by the day, even as organisations try to protect their data, using various known firewalls. The attacks have put some organisations out of business, while those that still survive, suffer huge financial losses regularly, especially in the financial services sector, where customers' accounts are targets of attacks.

Those involved in online hacking pay heavily to criminals to get information from the database of companies or they just aim at disturbing network operations by adding delays or even shutting down websites of competitor companies.

Many countries today are being attacked, and many cyber attacks come from China and Russia because there are no clear laws against cybercrime in those regions, though statements against it are pronounced in those countries. Most countries' data bases are encrypted, especially in the banking industries, corporate organisations, and government security agencies, but they are still targets for cyber criminals.

Millions of naira and dollars are lost due to frauds being perpetrated in the banking industry, which are mostly carried out by cyber criminals. It is on this premise that Palo Alto Networks, represented by Dizengoff West Africa Nigeria Limited, is introducing the most advanced solution that will detect and defend most advanced and unknown threats from cyber criminals.

About Cybercrime

The main goals of cyber criminals are to penetrate network, log in, and actively operate programs inside it, as well as remove sensitive data. They often use the information for terrorism, fraud, or commercial intelligence. In many cases, cybercriminals often target multiple sites and organisations to increase the spread of the virus.

They also use large numbers of remote infected computers to generate massive, synchronized, and orchestrated attacks on specific sites. When components in those networks crash, they penetrate the network.

With new variants of malware being generated on a daily basis, many companies struggle to fight these threats, and the majority of attacks are often left undetected or unreported.

Presently, cybercrime has advanced beyond just destroying a server or a component in a network and cyber criminals are looking constantly at new ways to attack.

In addition, cybercriminals are no longer isolated amateurs. Many belong to well-structured organizations, with money, motivation, and clear goals, often employing highly skilled hackers that execute targeted attacks. Such organisations can deploy considerable threat intelligence, time, and resources in order to execute attacks that can cost cybercrime victims money, property, and reputation.

The nature of applications is also changing. Some common applications use encryptions, hub porting, and other evasive

ways to ensure that their legitimate information will pass to the other side even against current protections measures that reside in the network.

Such are called application-shift in which the legitimate application without user intervention hops between different ports of the network, imitating other applications in order to pass by the barricades of traditional firewalls. Most of these applications are being used normally at offices by employees for daily work and for their social life.

At the same time unscrupulous individuals may use them for dishonest purposes as a conduit to lodge criminal attacks on the networks. Unfortunately, this trend is only growing more complex, as businesses experience a surge in application usage and more employees communicate via social media. Employees are also embracing mobile and cloud computing, creating more and more channels of communication and vulnerable entry points into networks.

Traditional Firewalls

Meanwhile, the use of traditional firewalls and other intrusion protection solutions which are port and protocol oriented to protect the networks, guard against old versions of cyber-attacks.

But experts have said that such blocking processes can no longer protect the network, because the traditional firewalls were built to protect the ports of the network and protocols and do not focus on the content that is presumably legitimate and is passing in and out of the network and can carry evasive programs.

According to the expert view, traditional firewalls also do not monitor the application running in the network and assume the network users act as they are "supposed to," meaning they have taken all security precautions in their activities.

Vulnerability of Nigerian Banks and Other Organisations

Cyber criminals are increasingly targeting fast growing economies, especially Nigeria, knowing that private sector enterprises and government agencies lack the same levels of experience, infrastructure and installed capabilities.

The banks networks are porous and exposed to cyber-attacks, and thus will need world class cyber resilience strategies, systems, solutions, and professionals simply because they are fast becoming the new targets of these very adept and smart globally based cyber criminals, cyber terrorists, and hackers, according to the experts' view.

They are of the opinion that global cyber criminals will always follow the money. Like any armed robber, they will choose to target those that may appear the least experienced or sophisticated in the cyber security protection me adopt. Nigeria is awash with new targets for ther know it.

The cyber criminals may also reside outside Nig dictions. In this new interconnected, digitally interac where the Internet of things now exist, in a few cyber criminals can penetrate poorly protected data centers and even sophisticated retail banking netwo devices as simple as a mobile phone, often from a the world, they said.

Predictions of Cyber Attack

With the evolution of cybercrimes and security th last year, experts have predicted that 2014 will be ar demanding year for security, based on renewed targe

This is a wake-up call for the enterprise to pla priority on proactive network technology strategy.

According to them, cyber criminals will target d and control systems that support infrastructure.

"We expect a significant increase in attacks w hackers target the weakest parts of a data center su structure. Many enterprises in both the public and pr in Nigeria have made strides at strengthening their security, but they are expected to do more," experts

The demand for cyber security skills will reach and the need to keep teams equipped with the righ be critical. Advanced threats have become commo the demands on existing incident response teams ha outstrip capacity, especially in enterprises and gover ties where cyber security skills are already in short said, adding that a recent survey concluded that only of security professionals felt they had the expertise with advanced threats.

Equally important, is investing in training an cyber security professionals by banks, blue chip state, and federal agencies. They should evaluate w equip their teams with security solutions that tru according to experts' view.

Solutions for Banks, Enterp Data Center Executives

The advancement and level of sophistication of re attacks indicate a critical need for Information (IT) practitioners to invest in network security including resources, training, and technology, to b for attacks.

Businesses should utilize the most up-to-date a configured devices and carefully plan the position o

within the network architecture. Additionally, organisations should examine their abilities to withstand prolonged, sophisticated attacks and estimate the resources required to thwart or mitigate such attacks.

By following best practices, organisations will have a significantly better chance of withstanding anticipated cyber threats. Traditional Firewalls and other security devices have been installed in most organisations in Nigeria but they have their disadvantages; they cannot handle modern cyber-attacks disguised as legitimate and they do not monitor and police the user and application running inside the network.

They also add a lot of delays to the information running in the network as each device processes in serial another parameter of the data, they look outside to protect the gateway into the network but do not protect what is running inside the site and this does not allow a panoramic view of all that is done in the network.

These are the views of Palo Alto Networks that recently introduced its advanced cyber solutions for the financial sector. The company is of the view that Nigerian organisations need the support of international organisations, considering what is involved, since cyber attacks have become a global issue.

Financial Losses

Organisations allover the world, including Nigeria do not reveal that they have suffered a cyber attack for fear of losing customers' confidence in their business.

But according to the 11th Annual Global Information Security Survey, conducted by PriceWaterhouseCoopers and CSO Online, executives remained confident in the robustness of their security initiatives. In the survey, 84 percent of Chief Executive Officers (CEOs) and 82 percent of Chief Information Officers (CIOs) contend their cyber security programs are effective, while 78 percent of Chief Information Security Officers express full confidence in their existing cyber security programs.

However, the Central Bank of Nigeria, in its annual report for 2012, had shown that the number of reported cases of fraud and forgery in the banking industry increased in 2012. According to the apex bank, there were 4,527 cases of fraud and forgery involving the sum of N14.8 billion and $1.6 million, compared with 2,527 cases involving the sum of N29.5 billion at the end of December 2011, but unfortunately the trend continues in 2013 and 2014.

Next-Generation Firewall

A modern architecture of network security solutions that controls the safe enablement of applications, and exceptional levels of protection by blocking all known threats operating across a multitude of different sectors and a next-generation threat, has been introduced by Palo Alto Network, a world-leading network security firm that is represented in Nigeria by Dizengoff West Africa Nigeria Limited.

According to the company, the solution enables quick discovery and elimination of previously unknown malware, zero-day exploits and advanced persistent threats. Dizengoff was appointed in 2013 by Palo Alto Networks as its distributor and support partner within Nigeria. Detecting and eliminating previously unknown threats across all applications is the key to protecting an organisation from today's advanced threats, the company said.

With the introduction of new solutions from Palo Alto Network, it is expected that organisations, especially banks, will record less financial losses from cyber attacks.

Critical Thinking

1. With new variants of malware being generated on a daily basis, is it feasible that companies such as Palo Alto Networks can keep pace? Why or why not?
2. Why are the banks and other organizations of Nigeria particularly susceptible to cybercrime?
3. Why do organizations throughout the world fail to reveal that they have suffered a cyber attack?

Create Central

www.mhhe.com/createcentral

Internet References

MarketWatch: "800 million Apple devices threatened by 'WireLurker' malware"

http://www.marketwatch.com/story/palo-alto-networks-says-new-malware-threatens-800-million-apple-devices-2014-11-06

New York Times: "The New Nigerian Email Swindle"

http://bits.blogs.nytimes.com/2014/07/22/the-new-nigerian-email-scam/?_r=0

Yahoo! News: "Palo Alto Networks discovers new malware targeted at Apple devices"

http://news.yahoo.com/palo-alto-networks-discovers-malware-targeted-apple-devices-002619441

Article

Prepared by: Caroline Shaffer We
California National University for Advanced

The Individual in a Networked World: Two Scenarios

Collaborative agent bots? A walled world under constant surveillance? Tw information technology experts parse the future of human–network intera

LEE RAINIE AND BARRY WELLMAN

Learning Outcomes

After reading this article, you will be able to:

- Understand that the technologies we innovate do not guarantee either a utopian or dystopian future; we have options in how we choose to create policy and institutions around those technologies.
- Articulate characteristics of both utopian and dystopian futures.
- Define and describe the "Triple Revolution."

One of the most useful and formal futurism exercises in recent years was the work in 2006–2007 of the Metaverse Roadmap project. It was driven by John Smart, Jamais Cascio, and Jerry Paffendorf, and originally conceived of as a brief for the future of the World Wide Web as it became three-dimensional.

Once the leaders of the effort began to hear from several dozen thinkers, their own views branched in other directions. They had started their inquiries with the notion of a "Metaverse" that was first conceived by the influential science-fiction writer Neal Stephenson in his 1982 classic, *Snow Crash*. To Stephenson, the Metaverse was an immersive, virtual space with 3-D technologies.

Yet, the Metaverse Roadmap thinkers went beyond seeing the Metaverse as a virtual domain. They saw it as the "convergence of (1) virtually enhanced physical reality and (2) physically persistent virtual space. It is a fusion of both, while allowing users to experience it as ei other words, it is the connection of the physical an worlds. Although we do not foresee people livin in virtual space, the technological directions sugg the Metaverse Roadmap provide guides for how ne individualism may proceed.

This is a future that has already come to pass respects. There is already a mad rush in Silicon Valley products to embed social interplay in most kinds of tion and media encounters, and it will likely accelera forward. Moreover, in coming years a wider Metav emerge as relatively ordinary objects—as well as c and phones—will become ubiquitously networked w other, and networked individuals will be able to augm information through direct contact with databases an that have become smarter and more communicative.

Increased computing power may make people's ments in virtual worlds more immersive and co although experiences to date suggest that people are to use computer networks that integrate with real li than becoming totally immersed in virtual worlds—wi game players the exception.

Ubiquitous computing, sometimes called "the In things" (or "everyware"), describes human–computer tion that goes beyond personal computing to an enviro objects processing information and networking with ea and humans. Objects would share information: ap utility grids, clothing and jewelry, cars, books, ho and workplace furnishings, as well as buildings a scapes. They would learn additional information and p

methods of use by gathering data about people who are in their environment. For example, cars could tell each other not to be in the same lane at the same time, and bicycles could tell car doors not to open suddenly when the bikes pass by.

With all these trends rolling along into the future, there is still reason to be uncertain about how the environment of networked individuals will evolve. We offer two different scenarios that seem credible.

Scenario 1: Collaborative Agents in Augmented Reality

Waking up in a networked future, his digital agent's soft voice slowly grows into Harry Sanchez's hearing range. It's been monitoring his sleep rhythms and cross-referencing them with data from his ongoing brain scans to see when it's most appropriate to wake him. After stretching and rubbing the sleep from his eyes, Harry suddenly and happily recalls yesterday's purchase.

He found a collaborative coupon on the Web the other day for a deal on a new pair of augmented reality (AR) contact lenses and the haptic feedback implant that everyone's been raving about. The implantation was a simple and quick outpatient procedure that reminded him more of getting his ears pierced than of surgery. It was performed remotely by a doctor whose robot mimicked his every move. It was not as though Harry could really tell, however, since his AR glasses had "skinned" (covered) the robot with the doctor's virtual image. In this way, the doctor efficiently treats dozens of patients a day, projecting in from his home.

Now that he is awake, Harry eagerly slips in his new AR contact lenses for the first time. They instantly network with his microcomputer, smartphone, and the Internet. His personalized augmented overlay appears in his field of vision: the time and date, the weather and air quality, a few applications he left open from the previous night minimized into his peripheral vision, a faintly blinking icon notifying him of some messages he missed overnight, an icon notifying him of information updates on news stories aggregated for him by his agent, and an InterFace lifelog update showing what his friends did last night that is cross-referenced with the media they consumed and the tagged conversations they had. He sees a call for participating in a political smart mob in the virtual world, but he tells his agent to disregard it.

His agent also warns him about his health.

Harry hasn't been sleeping well, as his late-night virtual meetings with colleagues in China have taken a toll on his system. Yet, he's happy to not have to fly there ever since they've been able to collaborate long-distance by using the Cavecat productivity system with active walls and tables holding spreadsheets, texts, drawings, and videos.

As Harry settles in at the kitchen table, the surface notices that he's put down his morning cup of coffee. Finally, the news displays as manipulable augmented reality overlays of Harry's social network, with pictures of each network member blinking when she or he posts messages, videos, or lifelog entries.

The new haptic implant gives him a sensory understanding of the news: He can feel the continuing battle in Kabul, experiencing its sounds and vibrations as if he were at the scene. And it now feels as if the computer icons of his various applications have weight and texture. Having not found any urgent messages, Harry's agent organizes his correspondence by topic and relevance. Noticing a conversation he had that he does not want many network members to see, Harry has his agent make the information private across his entire InterFace network. His agent also sends out a quick update to his entire network, letting them know his plans for the day.

Harry is distracted by a knocking sound. His agent informs him that his best friend, Neal, is projecting in for their regular weekend virtual breakfast.

Though Harry and Neal only live 50 kilometers apart, this is a nice way for them to check in on one another and spend some time together. Harry hasn't shaved, and so he puts on his shiny-face skin before he opens the virtual door. He uses his new haptic chip to get the sensation of shaking his friend's hand. It's a little strange at first, since there's nothing actually present to shake, but his nervous system responds as though he had reached out and touched someone.

Harry and Neal chat about how everyone who was at the pub's avatar party last night has shared recordings of the evening with friends. Their agents have already automatically tagged these recordings with relevant information about people and location. Avatar parties have become popular these days. Everyone dresses like their favorite game character; some even come looking like one another. It can be a lot of fun role playing like this, and the collected and tagged videos are highly amusing as people's voices, looks, and even smells can be altered in the virtual world.

After visualizing and flipping through these tags for mentions of his name, Harry updates the conversation file with some witty things he thought of after the fact, and his agent forwards the updates to the relevant people. He also tells his agent to delete information about last night's embarrassing ice-cube escapade at the avatar party, and to ask his friends to delete their versions.

Harry's agent softly chimes in just as he's saying goodbye to Neal, reminding him that he has to meet his sister Merril today. The agents settle on a place downtown. Harry projects himself into the restaurant's virtual space. The restaurant keeps a good online presence, with a nice menu, list of ingredients, health report, and real-time webcam view. It's local and the tables there get automatically reserved.

As Harry gets ready for the day, his agent presents him with a few clothing options. He decides to wear the new trousers suggested by his girlfriend, but calls up another app to make sure his sister would also approve. Harry's girlfriend had tagged the info to the trousers while doing some virtual window shopping and had a pair in his size set aside after asking his belt how big it was.

Not wanting to be late, Harry has his agent arrange a car for him through a collaborative consumption app that recognizes his high trust score. He rarely uses a car, as his fridge automatically schedules grocery deliveries. Slipping his microcomputer into his pocket, Harry goes to the car, has his agent set the restaurant's coordinates, and leans back to check his messages as the car pulls out.

Scenario 2: A Walled and Surveilled World

As Will Li rouses himself from sleep, he walks over to "his" computer to see what he's missed overnight. Truthfully, the computer isn't really his: He owns rights to its usage but isn't allowed to change its hardware or software, or else he'd void his warranty or break the law. His computer is really only an access point, as all his data is in the cloud, yet another thing that's owned—with all the data in it—by a big corporation. Before Will can reach for the cloud, the system completes its mandatory scan of his computer for viruses and copyright infringement.

The price of media access has also spawned its own subculture of media pirates. They usually meet in person, sharing miniature portable terabyte flash drives packed with music, TV shows, movies, e-books, and more. The pirates often get their "warez" from people who collected old computers from trash heaps, recycling centers, and garage sales. They've even developed a code language to arrange meet-ups, but Will hardly keeps up with the ever-evolving lingo.

Leaning over his morning coffee, Will dreams of how nice it would be to have a personal agent, but he's heard most are double agents that also report back to the authorities and sell information to corporations. And he doesn't like the way FaceWall is collecting all the information on him whenever he uses it. He also can't afford to hire the technician it would require to help him set up the devices and access all the fragmented networks of media sites, search engines, and social applications online. Each has a tricky "right to information" form to sign. So he's reduced his online presence to a minimum, trying to limit himself to good old-fashioned e-mails and avoid social media.

However, Will needs to use FaceWall today to find something. He's forced to wait thirty seconds to let the mandatory ad play. It has his picture in it. CoffeeCo must have bought a recent photo that tagged him on a friend's wall. Will notices that his system slows down as the massive data file from the a ment clogs up his bandwidth, but since the corporat more to guarantee themselves fast access, he endures t

It's almost ironic to see a return to the days of loadin since the amount of available bandwidth has only incre all that bandwidth is auctioned at sky-high prices or c a few companies. Finally finding the photo, Will learn not delete it because CoffeeCo now owns it. Perhaps h make sure no one ever uploads anything about hi though that would be difficult. Most people seem to pu these situations because they want to keep going onl assumes that from now on he'll get peppered with ads the tastes that FaceWall has observed online—both for for all those other 40-year-olds who became unemploy countries set up their own walled-off Internets, clain morality and national security demanded it.

Giving the situation further thought, Will starts to his friends' profiles, and finds that his sister Lorelei ing extra money by selling her personal inform FaceWall, including links to his profile. Maybe that's h feeCo found his photo. He'll ask her when they meet never do it again. You can never be quite sure of who's ing on you, only in this case it's not only the state aggregating organizations.

Will remembers from history class how, in the 19 Director J. Edgar Hoover had used his dossiers on the dys to keep power. Now, FaceWall has even more con sive dossiers on everyone. Doing what he knows he sh Will reaches for a doughnut. Maybe he can sneak one his insurance company's sensors registering it. At le made the right decision by paying extra for their privac Otherwise, his health data might have just been sold c highest bidder at an info auction. But, since he's not ab the information himself, he can't be sure.

Will and his best friend, Spider, prefer to meet in There is less chance for any number of things happeni remember how Spider was once duped by someone himself off as an online insurance representative to s vate information. The latest scam is reverse-identity th thieves pose as old friends, using detailed avatars whos image and voice have been reconstructed from public Too bad the government killed the trusted identities p Will shuts off the computer monitor, grabs his phone travel pass, and goes out past the security scanner.

After a wait, Lorelei pulls up, giggling about the wh security scan at the gate. "Hope they got a better pic time." She's also worried that maybe the guards had f incriminating photo of her online. She's already lost because of it, even though it was taken without her pe and out of context. They head off for their meal, but ar in time to see the last open table become occupied.

The Possible Futures of Networked Individuals

Although present technologies are still far from realizing either scenario in its entirety, each represents a potential evolution from current trajectories. The first scenario assumes a move toward more networked individualism based on continued technological progress and trust in computer and human networks—including the withering of boundaries.

The second scenario assumes more boundaries, more costs, more corporate concentration, and more surveillance. At present, the Western world is trending in the direction of the first scenario, but we would be naïve to think that the second scenario could not happen.

What we call the Triple Revolution—in social networks, in the Internet, and in mobile connectedness—will change but never end in the ongoing turn to a networked operating system. The foreseeable future holds the prospect that individuals will be able to act more independently with greater power to shape their lives, if they choose to do so and if the circumstances will enable them to do so.

Yet, the foreseeable future also contains the burden of knowing that people will have to work harder on their own to get their needs met. Tightly knit, permanent groups will continue to be stable cores for some, and social networks will play greater roles in all human activities. The work of networked individuals is never quite done—and the satisfactions of netweaving are always available.

Critical Thinking

1. What are the critical factors in our society that will determine where our actual future falls on the continuum between Rainie's and Wellman's utopia and dystopia? What will determine how those factors play out?
2. In reading the dystopian scenario two, which particular characteristic of this society troubled you the most? Why?
3. Rainie and Wellman refer to the "Triple Revolution," what is it? How is it related to the two extreme futures they portray?

Create Central

www.mhhe.com/createcentral

Internet References

Gary Kovacs: Tracking Our Online Trackers [TED Talk]
www.ted.com/talks/gary_kovacs_tracking_the_trackers.html

Marc Goodman: What Does the Future of Crime Look Like? [NPR Interview from TED Radio Hour]
www.npr.org/2013/09/13/215831944/what-does-the-future-of-crime-look-like

The Quantified Self: Data Gone Wild?
www.pbs.org/newshour/bb/science/july-dec13/quantifiedself_09-28.html

Tomorrow's World: A Guide to the Next 150 Years
www.bbc.com/future/story/20130102-tomorrows-world

Warning: Cover Up Your Webcam When Not in Use
http://techland.time.com/2013/06/20/warning-cover-up-your-webcam-when-not-in-use/?iid=obinsite

Lee Rainie is the director of the Pew Research Center's Internet & American Life Project, a nonprofit, nonpartisan "fact tank" that studies the social impact of the Internet. Prior to that he was the managing editor for *U.S. News & World Report*. He is delivering the opening plenary keynote at WorldFuture 2012, the annual conference of *the World Future Society, in Toronto, Canada, July 27–29. (http://www.wfs.org/worldfuture-2012).*

Barry Wellman directs the University of Toronto's NetLab, is a member of the Cities Centre and the Knowledge Media Design Institute, and is a cross-appointed member of the Faculty of Information. Wellman is a member of the Royal Society of Canada, chair-emeritus of both the Community and Information Technologies section and the Community and Urban Sociology section of the American Sociological Association, and a fellow of IBM Toronto's Centre for Advanced Studies.

Article

Prepared by: Caroline Shaffer W
California National University for Advanced

What Facebook Knows

The company's social scientists are hunting for insights about human behavior. What they find could give Facebook new ways to cash in on our data—and remake our view of society.

TOM SIMONITE

Learning Outcomes

After reading this article, you will be able to:

- Understand the depth of personal information stored by businesses on the Internet.
- Understand how and why Google, Facebook, and other sites collect demographic and behavioral data.
- Understand how social networking data can be monetized at both the personal and aggregate level.

Cameron Marlow calls himself Facebook's "in-house sociologist." He and his team can analyze essentially all the information the site gathers.

Few Privacy Regulations Inhibit Facebook

Laws haven't kept up with the company's ability to mine its users' data.

If Facebook were a country, a conceit that founder Mark Zuckerberg has entertained in public, its 900 million members would make it the third largest in the world.

It would far outstrip any regime past or present in how intimately it records the lives of its citizens. Private conversations, family photos, and records of road trips, births, marriages, and deaths all stream into the company's servers and lodge there. Facebook has collected the most extensive data set ever assembled on human social behavior. Some of your personal information is probably part of it.

And yet, even as Facebook has embedded itself ern life, it hasn't actually done that much with wh about us. Now that the company has gone public, t to develop new sources of profit is likely to force it with its hoard of information. That stash of data loo oversize shadow over what today is a modest onlir ing business, worrying privacy-conscious Web user such as Google. Everyone has a feeling that this unp resource will yield something big, but nobody knows

Even as Facebook has embedded itself into mo hasn't done that much with what it knows about u of data looms like an oversize shadow. Everyone ha that this resource will yield something big, but nob quite what.

Heading Facebook's effort to figure out what can from all our data is Cameron Marlow, a tall 35-year-ol recently sat a few feet away from Zuckerberg. The low runs has escaped the public attention that dogs founders and the more headline-grabbing features ness. Known internally as the Data Science Team, of Bell Labs for the social-networking age. The gr researchers—but is expected to double in size this apply math, programming skills, and social science t data for insights that they hope will advance Facebook and social science at large. Whereas other analysts pany focus on information related to specific onlin Marlow's team can swim in practically the entire oc sonal data that Facebook maintains. Of all the peop book, perhaps even including the company's lea researchers have the best chance of discovering wha be learned when so much personal information is c one place.

Facebook has all this information because it has found ingenious ways to collect data as people socialize. Users fill out profiles with their age, gender, and e-mail address; some people also give additional details, such as their relationship status and mobile-phone number. A redesign last fall introduced profile pages in the form of time lines that invite people to add historical information such as places they have lived and worked. Messages and photos shared on the site are often tagged with a precise location, and in the last two years Facebook has begun to track activity elsewhere on the Internet, using an addictive invention called the "Like" button. It appears on apps and websites outside Facebook and allows people to indicate with a click that they are interested in a brand, product, or piece of digital content. Since last fall, Facebook has also been able to collect data on users' online lives beyond its borders automatically: in certain apps or websites, when users listen to a song or read a news article, the information is passed along to Facebook, even if no one clicks "Like." Within the feature's first five months, Facebook catalogued more than five billion instances of people listening to songs online. Combine that kind of information with a map of the social connections Facebook's users make on the site, and you have an incredibly rich record of their lives and interactions.

"This is the first time the world has seen this scale and quality of data about human communication," Marlow says with a characteristically serious gaze before breaking into a smile at the thought of what he can do with the data. For one thing, Marlow is confident that exploring this resource will revolutionize the scientific understanding of why people behave as they do. His team can also help Facebook influence our social behavior for its own benefit and that of its advertisers. This work may even help Facebook invent entirely new ways to make money.

Contagious Information

Marlow eschews the collegiate programmer style of Zuckerberg and many others at Facebook, wearing a dress shirt with his jeans rather than a hoodie or T-shirt. Meeting me shortly before the company's initial public offering in May, in a conference room adorned with a six-foot caricature of his boss's dog spray-painted on its glass wall, he comes across more like a young professor than a student. He might have become one had he not realized early in his career that Web companies would yield the juiciest data about human interactions.

In 2001, undertaking a PhD at MIT's Media Lab, Marlow created a site called Blogdex that automatically listed the most "contagious" information spreading on weblogs. Although it was just a research project, it soon became so popular that Marlow's servers crashed. Launched just as blogs were exploding into the popular consciousness and becoming so numerous that Web users felt overwhelmed with information, it prefigured later aggregator sites such as Digg and Reddit. But Marlow didn't build it just to help Web users track what was popular online. Blogdex was intended as a scientific instrument to uncover the social networks forming on the Web and study how they spread ideas. Marlow went on to Yahoo's research labs to study online socializing for two years. In 2007 he joined Facebook, which he considers the world's most powerful instrument for studying human society. "For the first time," Marlow says, "we have a microscope that not only lets us examine social behavior at a very fine level that we've never been able to see before but allows us to run experiments that millions of users are exposed to."

Marlow's team works with managers across Facebook to find patterns that they might make use of. For instance, they study how a new feature spreads among the social network's users. They have helped Facebook identify users you may know but haven't "friended," and recognize those you may want to designate mere "acquaintances" in order to make their updates less prominent. Yet the group is an odd fit inside a company where software engineers are rock stars who live by the mantra "Move fast and break things." Lunch with the data team has the feel of a grad-student gathering at a top school; the typical member of the group joined fresh from a PhD or junior academic position and prefers to talk about advancing social science than about Facebook as a product or company. Several members of the team have training in sociology or social psychology, while others began in computer science and started using it to study human behavior. They are free to use some of their time, and Facebook's data, to probe the basic patterns and motivations of human behavior and to publish the results in academic journals—much as Bell Labs researchers advanced both AT&T's technologies and the study of fundamental physics.

It may seem strange that an eight-year-old company without a proven business model bothers to support a team with such an academic bent, but Marlow says it makes sense. "The biggest challenges Facebook has to solve are the same challenges that social science has," he says. Those challenges include understanding why some ideas or fashions spread from a few individuals to become universal and others don't, or to what extent a person's future actions are a product of past communication with friends. Publishing results and collaborating with university researchers will lead to findings that help Facebook improve its products, he adds.

Eytan Bakshy experimented with the way Facebook users shared links so that his group could study whether the site functions like an echo chamber.

For one example of how Facebook can serve as a proxy for examining society at large, consider a recent study of the notion that any person on the globe is just six degrees of separation from any other. The best-known real-world study, in 1967, involved a few hundred people trying to send postcards to a particular Boston stockholder. Facebook's version, conducted in collaboration with researchers from the University of Milan, involved the entire social network as of May 2011, which amounted to more than 10% of the world's population. Analyzing the 69 billion friend connections among those 721 million people showed that the world is smaller than we thought: four intermediary friends are usually enough to introduce anyone to a random stranger. "When considering another person in the world, a friend of your friend knows a friend of their friend, on average," the technical paper pithily concluded. That result may not extend to everyone on the planet, but there's good reason to believe that it and other findings from the Data Science Team are true to life outside Facebook. Last year the Pew Research Center's Internet & American Life Project found that 93% of Facebook friends had met in person. One of Marlow's researchers has developed a way to calculate a country's "gross national happiness" from its Facebook activity by logging the occurrence of words and phrases that signal positive or negative emotion. Gross national happiness fluctuates in a way that suggests the measure is accurate: it jumps during holidays and dips when popular public figures die. After a major earthquake in Chile in February 2010, the country's score plummeted and took many months to return to normal. That event seemed to make the country as a whole more sympathetic when Japan suffered its own big earthquake and subsequent tsunami in March 2011; while Chile's gross national happiness dipped, the figure didn't waver in any other countries tracked (Japan wasn't among them). Adam Kramer, who created the index, says he intended it to show that Facebook's data could provide cheap and accurate ways to track social trends—methods that could be useful to economists and other researchers.

Other work published by the group has more obvious utility for Facebook's basic strategy, which involves encouraging us to make the site central to our lives and then using what it learns to sell ads. An early study looked at what types of updates from friends encourage newcomers to the network to add their own contributions. Right before Valentine's Day this year a blog post from the Data Science Team listed the songs most popular with people who had recently signaled on Facebook that they had entered or left a relationship. It was a hint of the type of correlation that could help Facebook make useful predictions about users' behavior—knowledge that could help it make better guesses about which ads you might be more or less open to at any given time. Perhaps people who have just left a relationship might be interested in an album of ballads, or perhaps no company should associate its brand with the flo tion attending the death of a friend. The most valu ads today are those displayed alongside certain We because the searchers are expressing precisely what This is one reason why Google's revenue is 10 t book's. But Facebook might eventually be able to people want or don't want even before they realize i

Recently the Data Science Team has begun to us position to experiment with the way Facebook wo ing the site—the way scientists might prod an ant see how users react. Eytan Bakshy, who joined Fa year after collaborating with Marlow as a PhD stu University of Michigan, wanted to learn whether ou Facebook are mainly influenced by those of our cl who are likely to have similar tastes. That would sh the theory that our Facebook friends create an "ech that amplifies news and opinions we have already h So he messed with how Facebook operated for a billion users. Over a seven-week period, the 76 n that those users shared with each other were logge 219 million randomly chosen occasions, Faceboo someone from seeing a link shared by a friend. H this way created a control group so that Bakshy c how often people end up promoting the same lin they have similar information sources and interests.

He found that our close friends strongly sway v mation we share, but overall their impact is dwa collective influence of numerous more distant con sociologists call "weak ties." It is our diverse c weak ties that most powerfully determines what we're exposed to.

That study provides strong evidence against t social networking creates harmful "filter bubbl activist Eli Pariser's term for the effects of tuning t tion we receive to match our expectations. But th reveals the power Facebook has. "If [Facebook's] is the thing that everyone sees and it controls how is disseminated, it's controlling how information is society, and it's something we need to pay very cl to," Marlow says. He points out that his team hel understand what it is doing to society and publishes to fulfill a public duty to transparency. Another r which investigated which types of Facebook activit ple to feel a greater sense of support from their into the same category.

Facebook is not above using its platform to t behavior, as it did by nudging them to register as o Unlike academic social scientists, Facebook's emp a short path from an idea to an experiment on hund lions of people.

But Marlow speaks as an employee of a company that will prosper largely by catering to advertisers who want to control the flow of information between its users. And indeed, Bakshy is working with managers outside the Data Science Team to extract advertising-related findings from the results of experiments on social influence. "Advertisers and brands are a part of this network as well, so giving them some insight into how people are sharing the content they are producing is a very core part of the business model," says Marlow.

Facebook told prospective investors before its IPO that people are 50% more likely to remember ads on the site if they're visibly endorsed by a friend. Figuring out how influence works could make ads even more memorable or help Facebook find ways to induce more people to share or click on its ads.

Social Engineering

Marlow says his team wants to divine the rules of online social life to understand what's going on inside Facebook, not to develop ways to manipulate it. "Our goal is not to change the pattern of communication in society," he says. "Our goal is to understand it so we can adapt our platform to give people the experience that they want." But some of his team's work and the attitudes of Facebook's leaders show that the company is not above using its platform to tweak users' behavior. Unlike academic social scientists, Facebook's employees have a short path from an idea to an experiment on hundreds of millions of people.

In April, influenced in part by conversations over dinner with his med-student girlfriend (now his wife), Zuckerberg decided that he should use social influence within Facebook to increase organ donor registrations. Users were given an opportunity to click a box on their Timeline pages to signal that they were registered donors, which triggered a notification to their friends. The new feature started a cascade of social pressure, and organ donor enrollment increased by a factor of 23 across 44 states.

Marlow's team is in the process of publishing results from the last U.S. midterm election that show another striking example of Facebook's potential to direct its users' influence on one another. Since 2008, the company has offered a way for users to signal that they have voted; Facebook promotes that to their friends with a note to say that they should be sure to vote, too. Marlow says that in the 2010 election his group matched voter registration logs with the data to see which of the Facebook users who got nudges actually went to the polls. (He stresses that the researchers worked with cryptographically "anonymized" data and could not match specific users with their voting records.)

Sameet Agarwal figures out ways for Facebook to manage its enormous trove of data—giving the company a unique and valuable level of expertise.

This is just the beginning. By learning more about how small changes on Facebook can alter users' behavior outside the site, the company eventually "could allow others to make use of Facebook in the same way," says Marlow. If the American Heart Association wanted to encourage healthy eating, for example, it might be able to refer to a playbook of Facebook social engineering. "We want to be a platform that others can use to initiate change," he says.

Advertisers, too, would be eager to know in greater detail what could make a campaign on Facebook affect people's actions in the outside world, even though they realize there are limits to how firmly human beings can be steered. "It's not clear to me that social science will ever be an engineering science in a way that building bridges is," says Duncan Watts, who works on computational social science at Microsoft's recently opened New York research lab and previously worked alongside Marlow at Yahoo's labs. "Nevertheless, if you have enough data, you can make predictions that are better than simply random guessing, and that's really lucrative."

Doubling Data

Like other social-Web companies, such as Twitter, Facebook has never attained the reputation for technical innovation enjoyed by such Internet pioneers as Google. If Silicon Valley were a high school, the search company would be the quiet math genius who didn't excel socially but invented something indispensable. Facebook would be the annoying kid who started a club with such social momentum that people had to join whether they wanted to or not. In reality, Facebook employs hordes of talented software engineers (many poached from Google and other math-genius companies) to build and maintain its irresistible club. The technology built to support the Data Science Team's efforts is particularly innovative. The scale at which Facebook operates has led it to invent hardware and software that are the envy of other companies trying to adapt to the world of "big data."

In a kind of passing of the technological baton, Facebook built its data storage system by expanding the power of open-source software called Hadoop, which was inspired by work at Google and built at Yahoo. Hadoop can tame seemingly impossible computational tasks—like working on all the data Facebook's users have entrusted to it—by spreading them across many machines inside a data center. But Hadoop wasn't built with data science in mind, and using it for that purpose requires specialized, unwieldy programming. Facebook's engineers solved that problem with the invention of Hive, open-source software that's now independent of Facebook and used by many other companies. Hive acts as a translation service, making it possible to query vast Hadoop data stores using relatively simple code. To cut down on computational demands, it can

request random samples of an entire data set, a feature that's invaluable for companies swamped by data. Much of Facebook's data resides in one Hadoop store more than 100 petabytes (a million gigabytes) in size, says Sameet Agarwal, a director of engineering at Facebook who works on data infrastructure, and the quantity is growing exponentially. "Over the last few years we have more than doubled in size every year," he says. That means his team must constantly build more efficient systems.

One potential use of Facebook's data storehouse would be to sell insights mined from it. Such information could be the basis for any kind of business. Assuming Facebook can do this without upsetting users and regulators, it could be lucrative.

All this has given Facebook a unique level of expertise, says Jeff Hammerbacher, Marlow's predecessor at Facebook, who initiated the company's effort to develop its own data storage and analysis technology. (He left Facebook in 2008 to found Cloudera, which develops Hadoop-based systems to manage large collections of data.) Most large businesses have paid established software companies such as Oracle a lot of money for data analysis and storage. But now, big companies are trying to understand how Facebook handles its enormous information trove on open-source systems, says Hammerbacher. "I recently spent the day at Fidelity helping them understand how the 'data scientist' role at Facebook was conceived . . . and I've had the same discussion at countless other firms," he says.

As executives in every industry try to exploit the opportunities in "big data," the intense interest in Facebook's data technology suggests that its ad business may be just an offshoot of something much more valuable. The tools and techniques the company has developed to handle large volumes of information could become a product in their own right.

Mining for Gold

Facebook needs new sources of income to meet investors' expectations. Even after its disappointing IPO, it has a staggeringly high price-to-earnings ratio that can't be justified by the barrage of cheap ads the site now displays. Facebook's new campus in Menlo Park, California, previously inhabited by Sun Microsystems, makes that pressure tangible. The company's 3,500 employees rattle around in enough space for 6,600. I walked past expanses of empty desks in one building; another, next door, was completely uninhabited. A vacant lot waited nearby, presumably until someone invents a use of our data that will justify the expense of developing the space.

One potential use would be simply to sell insights mined from the information. DJ Patil, data scientist in residence with the venture capital firm Greylock Partners and previously leader of LinkedIn's data science team, believes Facebook could take inspiration from Gil Elbaz, the inventor of Google's AdSense ad business, which provides over a quarter of Goog
He has moved on from advertising and now runs a
startup, Factual, that charges businesses to acces
fully curated collections of data ranging from res
tions to celebrity body-mass indexes, which
collects from free public sources and by buying
sets. Factual cleans up data and makes the result a
the Internet as an on-demand knowledge store to
software, not humans. Customers use it to fill in
their own data and make smarter apps or services;
Facebook itself uses Factual for information ab
locations. Patil points out that Facebook could b
source in its own right, selling access to informat
from the actions of its users. Such information, h
be the basis for almost any kind of business, such
ing or charts of popular music. Assuming Faceb
this step without upsetting users and regulators
lucrative. An online store wishing to target its pr
example, could pay to use Facebook as a source
about which brands are most popular in which pl
the popularity of certain products changes through

Hammerbacher agrees that Facebook could sel
ence and points to its currently free Insights servi
tisers and website owners, which shows how the
being shared on Facebook. That could become
useful to businesses if Facebook added data obtai
"Like" button tracks activity all over the Web, or
data or information about what people read on the
precedent for offering such analytics for a fee:
2011 Google started charging $150,000 annually f
version of a service that analyzes a business's Web

Back at Facebook, Marlow isn't the one who
sions about what the company charges for, even if
shape them. Whatever happens, he says, the prin
his team is to support the well-being of the people
Facebook with their data, using it to make the ser
Along the way, he says, he and his colleagues
humanity's understanding of itself. That echoes
often doubted but seemingly genuine belief that Fa
is to improve how the world communicates. Just
exactly what that will entail. "It's hard to predict
go, because we're at the very early stages of this s
Marlow. "The number of potential things that we
Facebook's data is enormous."

Critical Thinking

1. The article states that the manager in charge of m
all the personal data Facebook collects believes t
revolutionize the scientific understanding of why
behave as they do. Do you think this understandi

Article

Prepared by: Caroline Shaffer V
California National University for Advance

Google's European Conundrum: Wh Does Privacy Mean Censorship?

Though Google is a U.S. company, its American rights don't transpose across the pond. A court case will determine whether Google has to comply with EU law, which could have far-reaching consequences for European users.

ZACK WHITTAKER

Learning Outcomes

After reading this article, you will be able to:

- Understand how data placed on the Internet is virally replicated in a manner that no one entity can control it, let alone erase it.
- Articulate how information available on the Internet impacts the trade-off of concerns between free speech rights and privacy rights.
- Know the risks of maintaining an online presence.

How Google and other American Internet companies operate in Europe could come down to a link that, depending on what side of the Atlantic Ocean you're on, should or should not be deleted.

A case heard Tuesday before the European Court of Justice (ECJ) hinges on a complaint submitted by a Spanish citizen who searched Google for his name and found a news article from several years earlier, saying his property would be auctioned because of failed payments to his social security contributions.

Spanish authorities argued that Google, other search engines, and other Web companies operating in Spain should remove information such as that if it is believed to be a breach of an individual's privacy. Google, however, believes that it should not have to delete search results from its index [http://www.reuters.com/article/2013/02/26/us-eu-googledataprotection-

it in the first place. Google argued that it is the responsibility and that its search engine is merely others' content.

The ECJ's advocate-general will publish its op case on June 25, with a judgment expected by th year. The outcome of the hearing will affect not on also all of the 27 member states of the European U

In principle, this fight is about freedom of s privacy, with a hearty dash of allegations of cens in. In reality, this could be one of the greatest ch privacy rules in decades—by either strengthening negating them altogether.

The European view is simple: If you're at o have to play by our rules. And in Europe, the "ri gotten" is an important one.

"Facebook and Google argue they are not subje as they are physically established outside the EU. Commission spokesperson told CNET. In new law proposals, the message is, "as long as a co its goods or services to consumers on the EU terr must apply."

While Europe has some of the strongest data p privacy laws in the world, the U.S. doesn't. And has some of the strongest free speech and expre the world, enshrined by a codified constitution, m countries do not, instead favoring "fair speech" pr

Google is also facing another legal twist: Spani are treating it like a media organization without full legal protection of one.

The European view is simple: If you're at our party, you have to play by our rules. And in Europe, the "right to be forgotten" is an important one.

Newspapers should be exempt from individual takedown requests to preserve freedom of speech, according to Spanish authorities, but Google should not enjoy the same liberties, despite having no editorial control and despite search results being determined by algorithms. Though Google is branded a "publisher" like newspapers, the search giant does not hold media-like protection from takedowns under the country's libel laws. This does not translate across all of Europe, however. Some European member states target newspapers directly and are held accountable through press regulatory authorities in a bid to balance freedom of speech and libel laws.

One of Spain's highest courts, the Agencia Espanola de Proteccion de Datos (AEPD), found in favor of the complainant in early 2011 and ruled that Google should delete the search result [http://online.wsj.com/article/SB10001424052748703396604576087573944344348.html]. This case is one of around 180 other ongoing cases in the country.

Google appealed the decision and the case was referred to the highest court in Europe, the ECJ, which will eventually determine if the search giant is the "controller" of the data or whether it is merely a host of the data.

The case will also decide on whether U.S.-based companies are subject to EU privacy law, which may mean EU citizens have to take their privacy cases to U.S. courts to determine whether Google is responsible for the damage caused by the "diffusion of personal information."

In a blog post on Tuesday [http://googlepolicyeurope.blogspot.com/2013/02/judging-freedom-of-expression-at.html], Bill Echikson, Google's "head of free expression," said the search giant "declined to comply" with a request by Spanish data protection authorities, as the search listing "includes factually correct information that is still publicly available on the newspaper's Web site."

"There are clear societal reasons why this kind of information should be publicly available. People shouldn't be prevented from learning that a politician was convicted of taking a bribe, or that a doctor was convicted of malpractice," Echikson noted.

"We believe the answer to that question is 'no'. Search engines point to information that is published online—and in this case to information that had to be made public, by law. In our view, only the original publisher can take the decision to remove such content. Once removed from the source webpage, content will disappear from a search engine's index."

EU's Latest Privacy Proposal: The "Right To Be Forgotten"

Should the ECJ find in favor of the Spanish complainant, it will see the biggest shakeup to EU privacy rules in close to two decades and would enable European citizens a "right to be forgotten."

In January 2011, the European Commission lifted the lid on draft proposals for a single one-size-fits-all privacy regulation for its 27 member states. One of the proposals was the "right to be forgotten," empowering every European resident the right to force Web companies as well as offline firms to delete or remove their data [http://www.cnet.com/8301-1009_3-57363585-83/new-eu-dataprotection-rules-due-this-week/] to preserve their privacy.

For Europeans, privacy is a fundamental right to all residents, according to Article 8 of the European Convention of Human Rights, in which it states [http://www.hri.org/docs/ECHR50.html#C.Art8]: "Everyone has the right to respect for his private and family life, his home and his correspondence." It does however add a crucial exception. "There shall be no interference by a public authority with the exercise of this right except . . . for the protection of the rights and freedoms of others."

Because U.S.-based technology giants like Google, Facebook, and Twitter have users and in many cases a physical presence in Europe, they must comply with local laws. The "right to be forgotten" would force Facebook and Twitter to remove any data it had on you, as well as Google removing results from its search engine. It would also extraterritorially affect users worldwide outside the European Union who would also be unable to search for those removed search terms.

Such Web companies have said (and lobbied to that effect) [http://www.telegraph.co.uk/technology/news/9070019/EU-Privacy-regulations-subject-to-unprecedented-lobbying.html] that the "right to be forgotten" should not allow data to be removed or manipulated at the expense of freedom of speech. This, however, does not stop with republished material and other indexed content, and most certainly does not apply to European law enforcement and intelligence agencies.

Two Continents, Separated by "Free" and "Fair Speech"

The U.S. and the EU have never seen eye-to-eye on data protection and privacy. For Americans and U.S.-based companies, the belief is that crossover between freedom of speech and privacy overlaps in "a form of censorship," according to Google's lawyers [http://www.bbc.co.uk/news/technology-12239674] speaking during the Spanish court case.

In the U.S., you can freely say the most appalling words, so long as they don't lead to a crime or violence against a person or

a group of people. In European countries such as the U.K. words can lead to instant arrest. Europe's laws allow for "fair speech" in order to prevent harassment, fear of violence, or even alarm and distress. It's a dance between the American tradition of protecting the individual and the European tradition of protecting society.

Google is fundamentally so very American in this regard. That said, Google already filters and censors its own search results at the behest of governments and private industry, albeit openly and transparently [http://www.google.com/transparencyreport/]. Google will agree to delete links that violate copyrights under the Digital Millennium Copyright Act, which seeks to remove content from Google's search results that may facilitate copyright infringement.

Google also complies, when forced by a court, with numerous types of government requests, not limited to subpoenas, search warrants, and National Security Letters [http://www.zdnet.com/what-google-does-when-a-government-requests-your-data-7000010418/], or so-called 'gagging orders'. It also discloses those requests and when it complies with them. And it's a system not that dissimilar to what it's being asked to do in Europe.

Whose Jurisdiction Is Google Under: U.S., EU, or Both?

While Europe's privacy principles apply to the Web, it's unclear whether they apply to data "controllers" established outside of the European Union. But several European court cases have sided with local law. A German court found that Facebook fell under Irish law [http://www.bloomberg.com/news/2013-02-15/facebook-scores-win-in-legal-regime-dispute-with-germany.html] because the social networking company had a physical presence in Ireland, another EU member state. In Google's case, Spanish authorities are making a similar argument, claiming that Google is processing data in a European state and therefore EU law should apply.

Many American companies have voiced their objections to the proposed EU privacy law [http://www.zdnet.com/blog/london/european-draft-data-law-announced-what-you-need-to-know/2609], including Amazon, eBay, and Yahoo, according to a lobbying watchdog [http://www.lobbyplag.eu/#/compare/overview]. It could still take a year or two for the law to be ratified.

"Exempting non-EU companies from our data protection regulation is not on the table. It would mean applying double standards," said Europe's Justice Commissioner Viviane Reding, the top politician in Europe on data protection and privacy rules in the region, in an interview with the *Financial Times of London* [http://www.ft.com/intl/cms/s/0/903b3302-7398-11e2-bcbd-00144feabdc0.html#axzz2MCRmwDfo].

The new EU Data Protection Regulation, proposed by the European Commission and currently being debated in the European Parliament, will likely be voted on by June.

But this fight isn't as much about censorshi think. It's about a cultural difference between and perspectives on what freedom of speech can It's also about privacy, and whether privacy or more important.

Critical Thinking

1. Explain why it is so difficult to completely rem tion placed on the Internet.
2. Assuming it were technologically feasible to co remove information from the Internet, should a be permitted to selectively remove information Internet about himself or herself? Should a priv permitted to do so? Should someone under 18 to do so? What about someone who had embar information posted with their consent?
3. Should a potential employer be permitted to sif old Internet information when making an empl decision? Should an existing employer be perm and potentially terminate an employee? Should spouse be able to look? Should a potential first answers are split between yes and no, what ger should guide when a historical search is approp when it is not?

Create Central

www.mhhe.com/createcentral

Internet References

California "Eraser Law" Lets Minors Remove Er Online Content
www.pbs.org/newshour/rundown/2013/09/californ minors-remove-embarrassing-online-content.html

EU Report: The "Right To Be Forgotten" Is Tech Impossible . . . So Let's Do It Anyway
www.techdirt.com/articles/20121205/08425221239/eu forgotten-is-technically-impossible-so-lets-do-it-anyway.sh

Juan Enriquez: Your Online Life, Permanent as a [TED Talk]
www.ted.com/talks/juan_enriquez_how_to_think_abo tattoos.html

Reputation 3.0: The Internet Is Your Resume
www.forbes.com/sites/dorieclark/2013/07/19/reputation-3-0-the-internet-is-your-resume

Survey: One-Third of Youths Engage in Sexting
www.wired.com/threatlevel/2009/12/sexting-survey

Temporary Social Media
www.technologyreview.com/featuredstory/513731/ten media

ZACK WHITTAKER writes for ZDNet, CNET and based in New York City.

Article

Prepared by: Caroline Shaffer Westerhof,
California National University for Advanced Studies

New Document Sheds Light on Government's Ability to Search iPhones

CHRIS SOGHOIAN AND NAOMI GILENS

Learning Outcomes

After reading this article, you will be able to:

- Understand how much personal information is embedded in the storage area of one's communcation and computing device.
- Recognize the tools that governments (and others) have to quickly and easily access information from communication devices.
- Recognize that U.S. Constitutional rights are limited at border crossings.

Cell phone searches are a common law enforcement tool, but up until now, the public has largely been in the dark regarding how much sensitive information the government can get with this invasive surveillance technique. A document submitted to court in connection with a drug investigation, which we recently discovered, provides a rare inventory of the types of data that federal agents are able to obtain from a seized iPhone using advanced forensic analysis tools. The list starkly demonstrates just how invasive cell phone searches are—and why law enforcement should be required to obtain a warrant before conducting them.

Last fall, officers from Immigration and Customs Enforcement (ICE) seized an iPhone from the bedroom of a suspect in a drug investigation. In a single data extraction session, ICE collected a huge array of personal data from the phone. Among other information, ICE obtained:

- call activity
- phone book directory information
- stored voicemails and text messages
- photos and videos
- apps
- eight different passwords
- 659 geolocation points, including 227 cell towers and 403 WiFi networks with which the cell phone had previously connected.

Before the age of smartphones, it was impossible for police to gather this much private information about a person's communications, historical movements, and private life during an arrest. Our pockets and bags simply aren't big enough to carry paper records revealing that much data. We would have never carried around several years' worth of correspondence, for example—but today, five-year-old emails are just a few clicks away using the smartphone in your pocket. The fact that we now carry this much private, sensitive information around with us means that the government is able to get this information, too.

The type of data stored on a smartphone can paint a near-complete picture of even the most private details of someone's personal life. Call history, voicemails, text messages and photographs can provide a catalogue of how—and with whom—a person spends his or her time, exposing everything from intimate photographs to 2 AM text messages. Web browsing history may include Google searches for Alcoholics Anonymous or local gay bars. Apps can expose what you're reading and listening to. Location information might uncover a visit to an abortion clinic, a political protest, or a psychiatrist.

In this particular case, ICE obtained a warrant to search the house, and seized the iPhone during that search. They then obtained a second, separate warrant based on probable cause before conducting a detailed search of the phone. However, even though ICE obtained a warrant for this cell phone search, courts are divided about whether a warrant is necessary in these circumstances, and no statute requires one. As a result, there are many circumstances where police contend they do not need a warrant

The police should not be free to copy the contents of your phone without a warrant absent extraordinary circumstances. However, that is exactly what is happening. Last year in California, for example, Governor Jerry Brown vetoed a common-sense bill that would have required the police to obtain a warrant before searching seized phones, despite the bill's broad bipartisan support in the state legislature.

Intrusive cell phone searches are becoming ever easier for law enforcement officers to conduct. Companies such as Cellebrite produce portable forensics machines that can download copies of an iPhone's "existing, hidden, and deleted phone data, including call history, text messages, contacts, images, and geotags" in minutes. This type of equipment, which allows the government to conduct quick, easy phone searches, is widely available to law enforcement agencies—and not just to federal agents.

While the law does not sufficiently protect the private data on smartphones, technology can at least provide some protection. All modern smartphones can be locked with a PIN or password, which can slow down, or in some cases, completely thwart forensic analysis by the police (as well as a phone thief or a prying partner). Make sure to pick a sufficiently long password: a 4 character numeric PIN can be cracked in a few minutes, and the pattern-based unlock screen offered by Android can be bypassed by Google if forced to by the government. Finally, if your mobile operating system offers a disk encryption option (such as with Android 4.0 and above), it is important to turn it on.

Critical Thinking

1. Read the *New York Times* and *The Atlantic Wire* web links at the end of this article about U.S. government searches at border crossings. Why do you think the gov granted more leeway at the border than Fourth ment protections against unwarranted search a normally provide? Do you think this extra leev appropriate? Why?
2. Describe the difference between data and meta the information stored on your cellphone. How be used to build a profile of the owner of a cell

Create Central

www.mhhe.com/createcentral

Internet References

The Border Is a Back Door for U.S. Device Searche
www.nytimes.com/2013/09/10/business/the-border-is-a-device-searches.html?pagewanted=all

Documents Reveal NSA Can Crack Online Enc Bastion of Privacy"
www.pbs.org/newshour/bb/government_programs/july-surveillance_09-06.html

4 Things You Should Know About Metadata, Hacke That Edward Snowden Would Never Tell You
www.forbes.com/sites/gregsatell/2013/08/03/4-thi know-about-metadata-hackers-and-privacy-that-edward never-tell-you

Here's How Phone Metadata Can Reveal Your Affa and Other Secrets
www.washingtonpost.com/blogs/the-switch/w heres-how-phone-metadata-can-reveal-your-affairs-abortions

When It's at the Border, Your Data Is Fair Game— Laptop
www.theatlanticwire.com/politics/2013/09/how-us-gover border-crossing-avoid-privacy-restrictions/69251