are less likely make errors or leave out important words and ideas if you slow down enough to write neatly.

- Whichever drafting option you choose, you should spend 15-20 minutes editing your paper. Check grammar, spelling, and clarity of language.
- Cite your sources: All borrowed material must be credited to the author whether you quote it directly or not. Remember to cite sources within the paper, and don't forget your Works Cited list on a separate page at the end of the essay.

Handling Test Anxiety

If you feel anxious or panicky while taking the WCT, try the following steps:

- Close your eyes.
- Take a long, deep breath.
- Concentrate on your breathing.
- Press your feet hard against the floor and count to five.
- Return to concentrating on your essay.

WCT Structure Sample Outline

Structure is extremely important to any essay or research paper, including the WCT. Good structure helps your reader follow your

discussion in the same way that good driving directions help you arrive at your destination without any wrong turns. There are many ways to structure a good essay, but several components are important:

- Division of paragraphs to show where each new idea starts
- Clear topic sentences which state the main point at the beginning of each paragraph
- Transitional words and phrases to show the progression of ideas and help the reader move smoothly from one idea to the next

The sample outline below shows one way to structure an essay:

Paragraph 1: Introduction

Begin your introduction with a general statement to reveal your topic. Then narrow the topic until you get to your main issue. State the thesis (your position on the issue) in one clear sentence at the end of the introduction.

Paragraph 2: Supporting point #1

- State the point clearly in your topic sentence
- Explain the point briefly to tell the reader what you mean

- Support the point with material from sources (quote or paraphrase) or with something from your own experience

Paragraph 3: Supporting point #2

- State the point clearly in your topic sentence
- Explain the point briefly to tell the reader what you mean
- Support the point with material from sources (quote or paraphrase) or with something from your own experience

Paragraphs 4: Supporting point #3

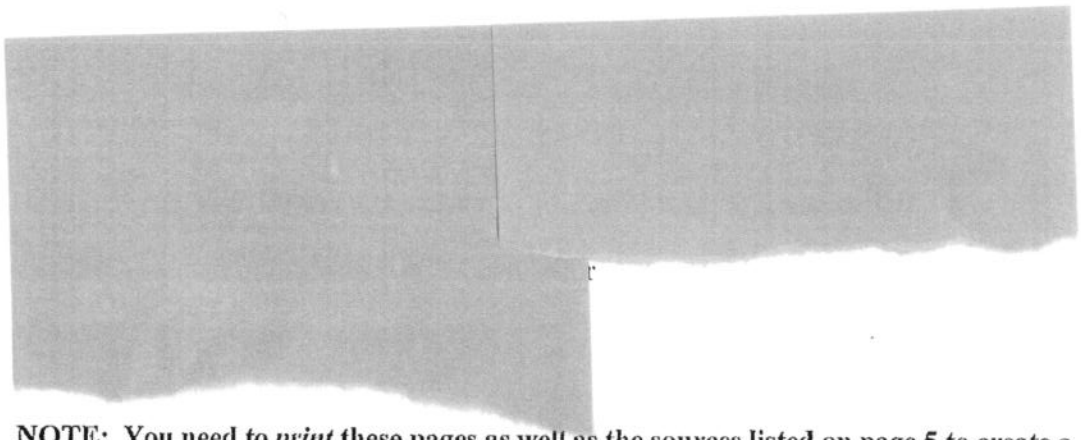
- State the point clearly in your topic sentence
- Explain the point briefly to tell the reader what you mean
- Support the point with material from sources (quote or paraphrase) or with something from your own experience

Paragraph 5: Conclusion

Bring the discussion back to the thesis and wrap it up

The format shown above may seem simple, and it is! Still, it is quite functional and will work with nearly any type of written piece from a five-paragraph essay to a much longer research paper.

It is usually helpful to outline before writing. Remember that it is permissible to have an outline written in your WCT packet when you



NOTE: You need to *print* these pages as well as the sources listed on page 5 to create a complete packet, in which you can take notes and bring to the Test.

THE SINGLE MOST IMPORTANT FACTOR IN PASSING THE WCT IS READING AND UNDERSTANDING THE MATERIAL ON THESE PAGES: THE COVER SHEETS, EVALUATION GUIDELINES, AND NOTE ON SOURCES.

FAILURE TO COMPLY WITH THE POLICIES AND PROCEDURES SPECIFIED BELOW MAY RESULT IN AUTOMATIC DISQUALIFICATION.

These are the materials for the next Writing Competency Test. A fee of $25.00 is assessed for *each* administration of the test, to cover administration and scoring costs. You should bring pens, an I.D., and a paid WCT fee receipt to the test. You may use erasable ink but *not pencil*. **Passing the Writing Competency Test is a University-wide requirement and a prerequisite for EN306 and equivalent courses.**

To prepare for the test, you should study the attached materials. They include

- the assessment scale that will be used by test evaluators. You should read it carefully so that you will have a clear idea of the criteria by which your test will be scored. Two evaluators will score each test.

- a selection of materials to ***print out*** , read, and consider for planning your essay.

For the test, you will be asked to write a critical essay on some point or idea discussed in the packet or suggested by it. Your essay should be clearly and significantly related to the packet material. There are many possibilities; you will need to develop your own topic.

Your essay must make at least some use of all the articles in the packet, but it should not be a summary of the articles. Don't plod through them paragraph by paragraph; instead, use them to develop your claim. You decide how to use them: some might be discussed in detail and others only mentioned briefly.

You should, therefore, read the articles carefully and critically; think about and maybe discuss with others the ideas they contain. Here are some suggestions to help you focus your thinking:

- What topics are common to all the readings?
- Which issue or idea discussed in these articles do you find most interesting?
- What evidence or support from *your own experience* could you use to develop your essay?
- What evidence or support do the *readings* provide?

In defining a FOCUS and DEVELOPING your ideas (see the attached Evaluation Standards for the meaning of these terms), you may want to consider these questions as well:

- What social, political, or economic questions do you see raised by the articles? How do you respond to them?
- What value questions do you see raised? How do you respond to them? Can you articulate an arguable claim about these questions?
- Are there aesthetic or scientific dimensions to the issue that would be interesting to raise?

You may do any planning and prewriting you want, but you may not bring any prewriting or drafts with you to the test. You should bring *only* the printed packet of articles to the test, and you may make any notes you want on the pages of the packet, including an outline of your essay and your documentation of sources. You may *not* have substantial portions of the essay written in the packet. You must turn in the complete printed packet, with your name on it, when you complete the test. A dictionary will be provided for your use at the test site.

Note that everything you write *during* the test, including notes, outlines, and drafts, *must be written in the bluebook*. Only material *written in the bluebook* will be considered by the scorers. Do not insert or staple material into the bluebook. Please leave the bluebook intact—don't tear out pages.

NOTE. *Be prepared to document sources you quote, paraphrase, or cite. Your essay must refer in some way to all of the articles, and it must contain a Works Cited list and parenthetical references or some comparable form of documentation. Use* ***ONLY*** *material from the packet as sources for your essay.*

Remember that your essay may be DISQUALIFIED if you
(1) write on a topic with no significant connection to the packet material, or
(2) use sources—other than your own experience, of course—from outside the packet.
Please be careful in planning your essay.

WCT EVALUATION STANDARDS

Your WCT essay will be evaluated on four criteria. Each one will be scored separately, so that a strong score in one area may make up for a weak score in another, but the four scores must total at least 8. You must, in addition, get acceptable scores (2 or above) in at least three categories. Each essay will be scored by two readers; in the event of a conflict, a third reader will decide.

These are the categories; each one will be scored from 1 (lowest) to 4.

FOCUS. A 4 is awarded to a critical essay whose controlling idea seems not only clear but particularly thoughtful or imaginative.

A 3 indicates a focus that is clear and sustained throughout but that may not be especially original in light of the readings.

A 2 in this category, as in the others, indicates minimum competence: the focus is clear but commonplace or conventional.

If the piece cannot be considered a critical essay, either because it simply summarizes one or more of the articles or because its focus does not offer an arguable claim, it receives a 1 in this category.

DEVELOPMENT. A 4 is awarded to an essay that, whatever its length, seems to the reader to be a full discussion. It makes use of both material from all the supplied readings and also ideas, experiences, or information personally supplied by the writer. All the material is smoothly integrated and persuasively supports the essay's focus. The writer seems to be a thoughtful, critical reader of the sources with a genuine personal "voice."

A 3 indicates that the writer has incorporated all the source material both appropriately in terms of content and smoothly in terms of style, and has also contributed personal ideas and experiences to the discussion. The essay's focus is clearly supported.

A 2 in this category indicates an essay that makes at least some use of each of the readings and some other material to support its focus, though the use may not always be relevant, and the sources not discussed critically.

A 1 is given to an essay that makes no use of the sources, does not at least mention every article, whose use fails to provide coherent support for the essay's focus, or whose use consists of unmarked quotation (copying from the sources word-for-word).

ORGANIZATION

The 4 essay is not only easy to follow, its structure seems effortless because of smooth transitions and a convincing rhetorical pattern.

A 3 is awarded to the essay that has clear paragraphing and a logical sequence of topics.

A 2 essay is generally easy to follow, with reasonable paragraphing, though the discussion may wander briefly.

The 1 essay is difficult to follow, either because the sequence of topics is not logical, because it is repetitive, or because the paragraphing is not helpful.

MECHANICS

The 4 essay reads exceptionally smoothly, and the reader notices no errors in grammar, usage, punctuation, or spelling. The Works Cited list is complete, and there is appropriate internal documentation.

The 3 essay may contain an occasional problem in sentence structure or diction, but the reader is never seriously distracted. Documentation is complete.

In a 2 essay, there may be enough mechanical problems to distract the reader temporarily, but it is always possible to understand what the writer means. Documentation is essentially complete.

A score of 1 indicates either severe problems with sentence structure or word choice--severe enough so that the meaning is difficult or impossible to understand--or serious deficiencies in documentation--no Works Cited list or inadequate documentation of material within the essay.

You Are What You Click.

Authors: Auerbach, David (AUTHOR)

Source: Nation. 3/4/2013, Vol. 296 Issue 9, p27-34. 6p.

Document Type: Article

Subject Terms: *CONSUMER research
*TARGET marketing
*RIGHT of privacy
*INTERNET protocol address
*COOKIES (Computer science)
UNITED States

Company/Entity: GOOGLE Inc Ticker: GOOG

Reviews & Products: FACEBOOK (Web resource)

Abstract: The article discusses the use of aggregated consumer information collected through computer and Internet activity for target marketing purposes, focusing on the practice's implications for consumer privacy. According to the article, Internet Protocol addresses and web cookies store user information that can be used in microtargeting. Topics include the "AdWords" software program from the Internet services and search engine company Google Inc., the consumer data aggregation company Acxiom, the social networking website Facebook, and the U.S. Consumer Privacy Bill of Rights legislation.

ISSN: 0027-8378

Accession Number: 85582198

You Are What You Click

BY DAVID AUERBACH

Every few months there's a headline story about privacy violations committed by a high-profile online company, and the violations usually span the spectrum. Google was recently slapped with two fines: $22.5 million for tracking users of Apple's Safari browser, and $25,000 for impeding an FCC probe into a bizarre episode of alleged wireless data "sniffing." For some years now, the privacy policies of Facebook have been under investigation in Germany and the United States.

What's always missing from these stories is context. Accounts of privacy violations bubble through the news and stir public outrage, which is often followed by a backlash and occasionally a fine. But these stories rarely reveal the porous privacy lines of the digital realm, or whether other types of violations are being committed online, by companies other than the household names. The outrage is selective and the enforcements ad hoc. News stories about hacking, data sniffing and the like have become red herrings. They provide false assurances that, in the normal course of things, our privacy is not being invaded on the Internet, that our personal data is safe, and that we are anonymous in our online—and offline—activities.

But we aren't. "Privacy" and "anonymity" are being defined down, and single violations of individual privacy like hacking and identity theft, while aggravating, are trivial compared with efforts toward the comprehensive accumulation of data on every single consumer. The marketing industry is attempting to profile and classify us all, so that advertising can be customized and targeted as precisely as possible. Google, Facebook, Apple and thousands of lesser-known companies are making it their policy and business to profile us in detail, all in the hopes of crafting better sales pitches. For these companies, your value is expressed most often when you click on an ad, signaling that you're interested in the product being sold. But will you buy it? For those paying for the ads, your value depends on other factors: your socioeconomic class, your credit, your purchasing record.

The sort of consumer profiling that has become increasingly necessary for targeted marketing has yet to generate significant increases in revenue. However, even the modest success of "microtargeting" has been enough to encourage the collection of vast quantities of consumer data, which is cheap and easy to do with today's technology. There is no incentive to stop this activity; no law prohibits it, and the growing electronic data hoard will be very difficult to expunge. Big Brother is watching you, but he's no longer a dictator; instead, he's a desperate and persistent door-to-door salesman. Call him Big Salesman.

Big Salesman is engineering a far grosser violation of our privacy than most people suspect—not a single incident, but a slow, unstoppable process of profiling who we are and what we do, to be sold to advertisers and marketing companies. Information that we reveal about ourselves constantly every day in our online and offline actions has become valuable to those who collect and amass it. Because the value does not lie in any one piece of data but in its unification and aggregation, the data in sum is worth far more than its individual parts. Ticketmaster may know which concerts I've attended and Amazon may know which albums I've bought, but each company would benefit if it had the other's file on me. It's a slow death by a thousand clicks: thousands of people see you on the street every day and it does not feel like an invasion of privacy, but if one person follows you everywhere as you work, read, watch movies and do myriad other things, it becomes stalking. And so we are stalked in the pursuit of marketing optimization.

WHERE THE MONEY IS

The key data lesson of the Internet age is that the amount of data one possesses is just as important as the type. With enough data, it becomes possible to see patterns that one could never guess in isolation. Consider two contrasting examples: toothpaste and the flu.

David Auerbach, a software engineer, has written for the Times Literary Supplement, Bookforum, n+1 and Triple Canopy. *He blogs at Waggish.*

Google Flu Trends is an example of apparently beneficent data aggregation. By tracking when and where people are searching Google for terms related to the flu, flu symptoms and flu treatments, Google has been able to predict outbreaks of influenza before government agencies do, and has made it easier to track the path of a flu virus. In many First World countries, Google's predictions have correlated reasonably closely with subsequent government data. Only an entity with access to an enormous plurality of all Internet searches could achieve such accuracy in prediction.

The same goes for consumer data. If a marketer sees me buy toothpaste at a drugstore, that is not tremendously valuable information by itself. But if he knows my entire history of toothpaste purchases, including which brands I buy and how often, he can predict when I might need to buy toothpaste again, and whether I might be inclined to click on an ad directing me to a lower-cost brand, or to a store selling my usual brand at a cheaper price. If my dental insurer knew my toothpaste purchases, it could classify me as higher or lower risk and adjust my premiums and payments accordingly.

Google Flu Trends gauges collective tendencies among many people, but market research is oriented toward the individual. Targeting the right set of consumers has always been at the heart of advertising, but when web ads first appeared in the 1990s, their click-through rates quickly plummeted as users wised up; people stopped clicking on even the brightest banner ads. The revolution in Internet advertising did not come until 2000, when Google introduced its AdWords program, which allows anyone to bid for placement on ad spots that appear in response to searches for keywords. Google's system collected little to no data about a user; the ads were displayed based merely on the search query itself. Searching for "watches" generates watch ads, searching for "asbestos" generates ads for tort lawyers. The advertising model fortuitously avoided many of the privacy concerns that are emerging today, because the very nature of Google's business ensured that it would find out exactly what consumers wanted at the exact moment they wanted it: during the search.

Yet Google's system was dependent on its having a search engine—*the* search engine, in fact. Click-through rates for online ads not generated by search engines are considerably lower, and Google's success in search ads has not been replicated anywhere else. For comparison, consider that Google's gross revenue was $37.9 billion in 2011 (96 percent of it from advertising), while Facebook's was merely $3.7 billion. And search continues to make up nearly half of all Internet advertising revenues, with Google dominating its competitors. Thus the social revolution precipitated by Facebook has not yet amounted to a shift in advertising effectiveness—one possible reason for Facebook's drastic decline in share price following its IPO in May 2012.

Internet marketing companies that aren't Google can't observe people at the moment of search, but knowing more about their lives might help refine targeted advertising. And so it has: while microtargeting hasn't come close to matching Google's success, it appears to have increased click-through rates sufficiently that several industries have sprung up around profiling and targeting consumers for advertising.

THE INFORMATION PIPELINE

Consumer data is collected, assimilated, processed, resold and exploited by a leviathan encompassing hundreds, if not thousands, of companies playing dozens of roles: ad brokers, data exchanges, ad exchanges, retargeters, delivery systems, trading desks. Some of these companies are well-known: Google, Facebook, Apple, Twitter, Yahoo. Beyond these, there are far more obscure entities trying to collect similar data, but their web presence is minimal. Companies like Acxiom, BlueKai, Next Jump and Turn build up demographic profiles so that advertising can be targeted as precisely as possible.

Ironically, the activities of the big names are more mysterious than those of smaller companies you haven't heard of. The operations of Facebook, Google and Amazon encompass the end-to-end collection of data: aggregation, usage and targeting. With their own private data sets, they don't need to engage in transactions with, say, data exchanges. The greatest use to which they can put their data is internal.

If you know who the smaller companies are, it's somewhat easier to find out what they do than it is to know what Google or Facebook is doing with your data. That said, Facebook and Google may not be doing single-handedly what these other companies do collectively; for many reasons, both business- and image-related, their agendas are different. But any company with a sufficient amount of consumer data can replicate the working model of the advertising ecosystem, and that should be enough to raise alarms. The model, though complex, breaks down into four stages through which consumer information is obtained and put to use: observation, collection, aggregation and targeting.

OBSERVATION

Whenever you browse the web, you leave a permanent trace of your activity. Every machine and device connected to the Internet has an IP address. The IP address does not identify you, but neither is it wholly anonymous. Blocks of IP addresses are associated with particular Internet service providers (ISPs), and most are geographically specific. This information is public: by visiting a website, you enable the website owner to learn where you are located. An ISP may assign you a different IP address over time, but frequently the address remains the same, so repeat visits can also be tracked.

Cookies are little pieces of data that websites ask your web browser to store. They can contain almost any data, but they're frequently used for remembering user preferences: the language you speak, for example, or your login and password. They also provide an easy way to tell when the same user is returning to a site. Browsers will send cookies back only to the site that sent them, and there are few limitations on what the site does with that knowledge, such as sell it to any or many other companies.

Companies like BlueCava have figured out a way to track online behavior without cookies. BlueCava's device identification platform attempted to identify individual users based on which browser and device they were using, information that is sent along with every request to a web server. (BlueCava now describes the service it provides as "multi-screen identification capabilities," presumably because it's harder to decipher what that actually means.) This is one of the reasons privacy remedies focused on particular technical mechanisms, such as the (mostly ignored) "do not track" header or third-party cookies, cannot suffice on their own.

The situation is different with sites like Facebook and Twitter, which require users to sign up for an account that they are encouraged to remain logged in to. Unless you micromanage your web privacy settings and browser activity, these sites have the ability to track you across the web. Every time you go to a site that has a Facebook "like" button or a Twitter "tweet" button or a Google "+1" button, or a site that lets you comment with your Facebook or Twitter or Google account, those companies know that you've visited the site, whether or not you click on the button. And every time you click the "like" button or authorize an application, Facebook eagerly hands over your data to the online gaming company Zynga, and to newspapers and publishing companies. Sharing your information with a third-party application on Facebook is

akin to poking a hole in a water balloon: only one prick is needed for everything to leak out.

COLLECTION

The lie of the web is that each page is a discrete entity. This was true a generation ago, when pages were merely formatted text, but now that they host all sorts of code and cookies, it's more accurate to think of web pages as collages of content, advertisements, federated services and tracking mechanisms that can talk to one another to a lesser or greater degree depending on your browser's privacy settings. The web is becoming a tightly connected mass of trackers and bugs, a single beast with a million eyes pointing in every direction.

If you're logged in to Facebook, Twitter, Google or Amazon, it's safe to say these sites are tracking and retaining everything you're doing on their sites and on any other sites that host their scripts and widgets. It's how they make recommendations: for friends, products, events. Advertising targeters like Acxiom, Turn and BlueKai are tracking users in a different though equally invasive way. A newspaper's website may know all the visitors to its site, but it knows nothing about their activities elsewhere. Its advertisers might, however, and Google Analytics certainly does: it offers a wide array of services to websites, tracking where users are coming from and what they search for before arriving at a page, all behind a slick interface. In exchange, Google gets to see the entire history of a site's access logs. Google Analytics and similar services like Quantcast and comScore are so ubiquitous that most of your web browsing is likely captured by one or more of these companies. They don't have your name, but they have your IP address, rough physical location and a good chunk of your activity online. This "raw data" is considered quite sensitive, since many companies have policies against retaining it. Google, for example, boasts of anonymizing IP addresses after nine months and cookies after eighteen. But many more sites lack any such policy, and few websites will promise that your visit has not been permanently archived by some unaffiliated company.

AGGREGATION AND MICROTARGETING

With so many entities collecting data and amassing consumer profiles, the profiles are often incomplete or even inaccurate. Acxiom may slot you, without your name, into a particular demographic: upscale young single male, suburban mom in a rich county, or one of many other categories. But for targeting coupons, a company needs far more than just a demographic. It needs to know which products you buy, the brands you like, when you buy and how.

This is the world of microtargeting. It has been used and refined over the last decade by political parties to determine where their voters are, so they don't mistakenly encourage the wrong people to get out and vote on Election Day. In 2012, the Obama campaign took a huge leap forward in microtargeting; its technology was unmatched by that of the inept Romney campaign, giving Obama's team a crucial edge in its ground game.

But identifying political affiliation is low-tech compared with advertising targeting, which needs to predict far more than one kind of behavior. Last June, *The New York Times* published a long article by Natasha Singer on Acxiom, which claims to have profiled 500 million consumers and offers its data in aggregated form to anyone who will pay for it, from websites to banks to insurance companies, and even to a US Army contractor. In the name of "multichannel marketing"—which is code for tracking a consumer in all her activities, from web browsing to television advertising to mail-order catalogs—Acxiom has been aggregating consumer data since its founding in 1969, and the explosion of data in the Internet age has been a big boon to it.

Acxiom is hardly an isolated actor, though. BlueKai claims to have profiled more than 160 million consumers, and in 2011 international advertising monolith WPP/GroupM started its own data aggregation division, Xaxis, which already claims to have amassed 500 million "unique consumer profiles." A Xaxis executive told *The Wall Street Journal* that this data would be obtained partly by purchasing it from companies like BlueKai. After some negative press, Xaxis has ceased bragging about that number and now speaks only in vague terms of customer reach. In November 2011, when Yahoo bought Interclick, now called Genome (which says it "aggregates and organizes billions of data points from third-party providers—delivering actionable consumer insights, scalable audiences and the most effective campaign execution"), the company was not just buying technology. It was also buying data.

Acxiom offers a lengthy and confusing form to opt out of its database, as well as the ability to see some of the data it has collected on you, though not for free: "Access to information about you in our directory and our fraud detection and prevention products will be provided in the form of a Reference Report that is available for a processing fee of $5."

To compensate for the limitations of their data sets, smaller sites are increasingly turning over their advertising operations to exchanges. An advertising exchange determines the user's identity and targeted demographic and then offers that knowledge to advertisers, who bid in real time for the opportunity to show the user their ad. The consumer may be identified generally as a member of a particular microdemographic, but because these "segments" are very small, they can be linked to personally identifiable information with ease. The exchange knows exactly who you are.

In these exchanges, decisions must be made faster than humans can make them—in fractions of an instant—and so complex algorithms are used to establish who "won" the bidding war to show a particular customer an ad. The real-time nature of the advertising ecosystem has reached levels of complexity reminiscent of automated derivatives trading and hedge funds, except that what is being traded are bets not on the future value of assets, but on the future value of consumer behavior: the likelihood that someone will click on an ad, use the coupon, buy the product.

Google launched its exchange, AdX, in 2009. Facebook recently launched the Facebook Ad Exchange, partnering with a number of companies with vague, mysterious names: Turn, TellApart, DataXu, MediaMath, AppNexus. (Turn, which claims to have 700 million consumer profiles through partnerships with Acxiom, eXelate, Facebook and others, sells placements based on the number of users within a particular "segment.") According to Bloomberg News, "Facebook Exchange will let advertisers reach specific types of users on the social network based on their browsing history."

Google and Facebook can be more secretive about their exchanges because everyone has tacit knowledge of what they have: millions of profiles of distinct users, reliably tracked by login. It remains to be seen how the third-party exchanges will compare. The ensuing partnerships will likely merge data sets, thereby enlarging the enormous consumer database that much more. And because the value of data increases the more it is aggregated, there is every incentive for third-party exchanges to enlarge their data sets through partnerships and acquisitions, either to compete with Google and Facebook, or to join them.

Companies like Turn sell themselves on their ability to reach microdemographics, and they are considerably less forthcoming about how effective such real-time targeting is, apart from selling advertisers on the idea that everyone is doing it and they should be, too. It's

possible that consumers aren't the only ones being manipulated: microtargeting seems to increase the effectiveness of advertising, but performing controlled experiments to gauge its impact is difficult. Sketchy evidence suggests that microtargeting raises click-through rates modestly, but falls short of doubling them. This is nothing compared to the advantage Google gained over its competitors when it launched AdWords. Nonetheless, the potential of microtargeting is indisputable, and for anyone who doubts the use of this data, there is the lesson of Google as a rejoinder: we just need more information, correlated with other data. The right combination of data, as Google found out, can be a gold mine

Last summer, DataXu co-founder Michael Baker wrote in *Forbes*, "It is no longer difficult to imagine a time in the not so distant future when all media—TV, radio, outdoor—is digital and addressable and capable of being purchased in an auction on an individual impression-by-impression basis." Baker is naturally speaking to advertisers, not consumers, who might find his vision rather alarming.

Microtargeting is not the only use being made of this data. Far more information has been collected than has been put to use, and the purposes to which it has been put have not always been visible to consumers. There is the danger of what law professor Frank Pasquale calls "runaway data," where personal data collected under one privacy policy is sold, resold or otherwise distributed so that deleting it becomes practically impossible. If this data is your personal profile, more than mere knowledge of your consumer habits can be gleaned. Two great dangers exist with runaway data: first, being put to more nefarious uses than coupon targeting; and second, the risk of deanonymization of consumer data, which establishes a link between anonymous data and a person's name. Both are enough to render any thought of personal privacy archaic.

Turn and other companies offer the ability to opt out of targeted advertising, and the "self-policing" group Network Advertising Initiative offers an opt-out promising that "the company or companies from which you opted out will no longer deliver ads tailored to your web preferences and usage patterns." In other words, they can still collect and sell data about you; they just won't use that data in one particular way.

The value of this consumer data is frequently thought to be in advertising, pure and simple, and viewed apart from the data-collecting methods undergirding it, advertising is comparatively innocuous: fine-grained targeting of online ads is creepy and invasive, but not dangerous.

Not so with other uses of that data. Consider credit ratings. Your FICO credit score is calculated by a secret formula. FICO has provided rough guidelines, saying it uses categories such as recent searches for your credit rating by third parties, but the company says nothing about what data is being used or where it comes from. There is nothing to prevent your Internet browsing activity from figuring into this calculation if credit bureaus are able to obtain it.

Things are worse with the less reputable "fourth bureau" credit agencies, which have been investigated by Ylan Mui in *The Washington Post*. These companies, such as L2C and LexisNexis, track people without a sufficient credit history to have files in the big three credit bureaus. Fourth bureaus do not follow the guidelines of the big three and have no disclosure regulations on what data they can use or any obligation to give it to you. Their information, as Mui discovered, is sometimes inaccurate, but you have no way of knowing that until their data results in your rejection for a job, an apartment or a loan.

Likewise, life and health insurance companies could have a field day with these files. A 2010 *Wall Street Journal* article described how Aviva's, AIG's and Prudential's life insurance arms were "exploring whether data can reveal nearly as much about a person as a lab analysis of their bodily fluids." Your profile can reveal all sorts of healthy or unhealthy tendencies: gym memberships, exercise equipment, bar tabs, poor diet, time spent on dating or hookup sites, an interest in recreational drugs. If you "like" the American Cancer Society or even Jack Daniel's on Facebook, for example, it won't just be advertisers who might take notice. And if there are any errors in your profile, you certainly won't have the chance to correct them, much less even know about them—you won't be told why your premiums are so high or your credit application was turned down.

Finally, there is the government. The National Security Agency, Department of Homeland Security and FBI already collect a tremendous amount of data on online activity, as Dana Priest and William Arkin revealed in *Top Secret America: The Rise of the New American Security State*. Some of the data, they found, was useful, but most of it was a vast stockpile of information on ordinary people, collected with a huge dragnet and permanently filed away because there was no pressing reason to delete it. Consumer profiles are ready-made grist for the national security mill. Companies like Google, Facebook and Twitter have sometimes resisted subpoenas for user information, but the chances that smaller, lower-profile marketing companies would stick their necks out by fighting a subpoena are slim. And you would not even know that your profile is being turned over to the government—you likely didn't even know it was being created.

Once your profile is created and passed around among companies, the circle of entities that know your behavioral patterns and day-by-day online and offline activity can only grow. This data is powerful, and though you had little to no say in its collection or sale, it is raw capital that can be put to use for the sake of profit in both benign and dangerous ways.

FALSE PROMISES OF PRIVACY

Promises of anonymity are misleading and far from absolute. In a famous 2000 study, Latanya Sweeney determined that a voter list could be correlated with medical records at a rate of 87 percent based not on any personal information but on three pieces of demographic data: sex, ZIP code and birth date. This allowed the "anonymized" medical data to be linked to a particular name.

But it is not just those three pieces of data: enough anonymous data of any form allows for a positive identification. In 2006, Netflix offered up a huge, seemingly anonymous data set of the complete video ratings of nearly half a million members. In their 2008 paper "Robust De-anonymization of Large Sparse Datasets," computer scientists Arvind Narayanan and Vitaly Shmatikov showed that very little knowledge was required to correlate one of the anonymous lists with an Internet Movie Database account: an overlap of even a half-dozen films between Netflix's list and an IMDb account could suffice to make a highly likely positive match. Because many IMDb accounts use people's real names and other identifying information, they provide a foothold for obtaining a person's entire viewing history.

A Netflix user history may seem like a fairly harmless example of "reidentification." Other data sets that are released "anonymously," including consumer purchases, website visits, health information and basic demographic information, appear more menacing. When AOL Research released a large data set of Internet searches for 650,000 users of AOL's search engine in 2006, *The New York Times* and others were immediately able to identify some of the users by finding personal information in the search queries. AOL admitted its error, but the data remains out there for anyone to view. Notoriously, there was User 927, whose searches included "beauty and the beast disney porn," "intersexed genitals," and "oh i like that baby. i put

on my robe and wizards hat."

In his 2010 paper, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization," law professor Paul Ohm wrote:

> Reidentification combines datasets that were meant to be kept apart, and in doing so, gains power through accretion: Every successful reidentification, even one that reveals seemingly nonsensitive data like movie ratings, abets future reidentification. Accretive reidentification makes all of our secrets fundamentally easier to discover and reveal. Our enemies will find it easier to connect us to facts that they can use to blackmail, harass, defame, frame, or discriminate against us. Powerful reidentification will draw every one of us closer to what I call our personal "databases of ruin."

Ohm's predictions are dire, yet his underlying point is irrefutable: both the value and the privacy of anonymized data are far higher than we intuitively think, because the data gains value only at large scale. The bits and pieces of this data we contribute, free and without compensation, become parts of large, profit-making machines.

Reidentification is a key aspect of giving value to data. It frequently has its value in the absence of total reidentification—marketers do not need to know your name or your Social Security number to show you ads. But if the value of the data goes up for credit bureaus and others that can determine your true identity, there is a strong incentive for them to do exactly that.

Hence, many privacy policies today give a false sense of security. Parsing the language of these policies is not easy, and because the information's value changes depending on how much other data it is collated with, such guarantees are at best naïve and at worst disingenuous.

As for subscription services, such as those offered by Apple, Google and Facebook, anonymity doesn't really exist. These companies already know who you are. Ex-Google CEO Eric Schmidt described the Google+ social network as fundamentally an "identity service" providing a verifiable "strong identity" for its users—one that requires you to use your real name. Needless to say, actions performed while logged in to this identity are far less anonymous than those performed under a pseudonym or when not signed in.

As long as you are signed in with an account from these respective services, there is nothing to prevent all actions taken on their sites from being associated with your account. By default, Google records your entire search history if you are logged in with a Google account. The organization Europe Versus Facebook, founded by law student Max Schrems, has publicized the extent of Facebook's data collection. With the help of EU laws, he obtained Facebook's internal record of him, a thousand-page dossier containing more or less everything he had ever done on Facebook: invites, pokes, chats, logins, friendings, unfriendings and so on. The accrual of all possible data—unabashedly personal data—is the industry standard. The restrictions, where they exist, are only on how that data is used.

FIGHTING THE FUTURE

Given the choice, most consumers would prefer that their information not be collected and aggregated. And so advertisers and data aggregators have treated them like the proverbial boiling frog: enticing them into an indispensible social or technological network, then slowly eliminating their choices. Regulations and advocacy have been consistently losing ground against the advertising behemoth.

By default, browser and mobile software provide little protection against the collection of their data. Simple but powerful browser extensions such as Disconnect and Ghostery prevent a great deal of tracking via cookies on PCs, but they are used only by a small fraction of consumers. And even such extensions can't prevent the many other forms of tracking, and mobile platforms do not permit their use. Privacy advocate Brian Kennish, the creator of Disconnect, stresses the lack of transparency in data collection and use: "We're trading information we don't even understand for Internet products. If we don't even know what's happening, it's hard to assess the risk."

Cases like the one the government brought against Google are irrelevant to the central privacy issues of the day. There is no legal or regulatory infrastructure set up to monitor the collection, aggregation and trading of consumer information. Certain forms of information, such as medical records, are cordoned off by privacy legislation such as HIPAA, but even these laws are no guarantee of anonymity, as it is easy to determine much about a person's health and medical history by looking at his everyday purchases and activities. In great enough quantities, collection and aggregation of nonconfidential information can violate privacy just as much as the disclosure of confidential information does.

Most resistance to this kind of aggregation has been purely reactive and not particularly effective. When the resistance has had any effect, it has played on momentary consumer outrage. Consider the case of Facebook Beacon, launched in 2007: the concept was that companies partnering with Facebook, which included eBay, Yelp, *The New York Times* and Blockbuster, would allow it to put an invisible "web bug" on their sites that would enable Facebook to see everything its users did on the partner sites and associate that activity with their Facebook accounts, whether or not they were logged in. If I purchased shoes from Zappos, for example, Facebook would post that information to my wall automatically, saying, "David just bought shoes from Zappos!" Facebook users were "opted" in to Beacon without being asked and had to manually turn it off.

There was a public outcry: Facebook users did not want their online activity automatically advertised to their friends. MoveOn started a petition, and a class-action suit was filed against Facebook and several partners. Facebook quickly made Beacon optional for users, requiring an explicit opt-in, and subsequently allowed people to turn it off completely. Two years later, in 2009, it shut down Beacon altogether because, when given a choice, very few people wanted to opt in to such a program.

But Facebook didn't abandon the goals of Beacon. Rather, it learned from its mistake, grasping that what frightened people most about Beacon was seeing their online behavior publicized without their consent. Through the use of "like" buttons, comment registration and third-party cookies, Facebook still monitors a large percentage of the online activity that Beacon was supposed to capture. It just doesn't publicize its actions.

This kind of two-step, where data is collected but the consumer is not notified, has become the norm in Internet commerce. The two-step works in other ways. Facebook has drastically weakened its privacy policies several times, most notably in 2009, 2010 and 2012, each time attempting to make more user information less private by default. (A brief timeline is available from the Electronic Frontier Foundation, which has worked diligently to raise consumer awareness.) Whenever there was a strong public protest, Facebook retreated, but not to its original position, thereby cooling critics' ire while still managing to raise the flame under the frog.

Facebook's case is an unusually visible one. Most companies have not had their data collection practices scrutinized so closely, if at all. Natasha Singer's *Times* article about

Acxiom raised eyebrows in Congress and at the FTC, but no action has been forthcoming: "self-policing" seems to be the order of the day, which is to say there's no order at all. Because consumers remain mostly in the dark about the activities of companies like Acxiom, there is far less pressure on them than there has been on Facebook—and even there, the pressure hardly seems to have made a difference. The Obama administration's Consumer Privacy Bill of Rights, issued in February 2012, sets out vague guidelines for control and transparency that are wholly out of touch with reality: corporations have so far yielded nothing to it, and the government has not pressed the point.

Legislatively, there are very few existing guidelines, partly owing to the difficulty in quantifying exactly what should be illegal: companies have been collecting this sort of data for years, so how would one justify criminalizing the collection of more of it? In *Steinberg v. CVS*, decided last year, CVS successfully fought off a Pennsylvania lawsuit over giving "anonymized" data to pharmacy companies and data brokers, because no legal protections were in place beyond the requirement of scrubbing people's names from the data. The concept of reidentification has not yet entered the legal domain—nor has the inevitability that the data will be combined with other data.

There are many legal issues to resolve, and the only impetus for change appears to be consumer education and outrage. But given the complexity and obscurity of data aggregation today, outrage occurs only when a company makes a public relations gaffe that's big, simple and visible enough for the media to latch on to. Even then, few people end up leaving Facebook. All of your friends are there, being watched and anonymized as they "friend" and watch you, all of them doing, in the words of Joseph Turow, "free labor in the interest of corporate profits." ■

In Our Orbit

My Lai Rules

by RICHARD KREITNER

Last March, after a US soldier methodically shot and killed sixteen Afghan civilians, Defense Secretary Leon Panetta repeated that hoariest of maxims, "War is hell." The saying is often attributed to Gen. William Tecumseh Sherman, whose Union troops blazed a path of total destruction from Atlanta to Savannah near the end of the Civil War. But because it conveniently obscures any sense of agency, the notion that war is hell has long provided cover for the most ghastly and gratuitous wartime acts. Responding to one veteran's outrage over American massacres of South Vietnamese civilians, an army officer replied that it is "indeed unfortunate...that some incidents occur within combat zones."

Yes, one can describe as hellish a war in which American soldiers forced a woman into a bunker and buried her alive; tied another to an armored vehicle and dragged her around her village; used unarmed civilians for target practice; mashed the head of a 5-year-old with a rifle butt; emptied an entire clip into a man fishing in a lake; mounted heads on pikes to terrify the villagers; threw a naked woman, presumably raped, onto a pile of nineteen other women and children, then sprayed them with M-16 fire. But to speak of some "indeed unfortunate" incidents that "occur" is obscene.

That's one of the lessons of *Kill Anything That Moves: The Real American War in Vietnam* (Metropolitan; $30), Nick Turse's rigorously documented compendium of US atrocities large and small, committed from the air and on the ground during that conflict. Based on new archival research and more than 100 interviews with veterans and Vietnamese, the book elaborates on the argument that Turse, a fellow at the Nation Institute, previously put forward in these pages ["A My Lai a Month," December 1, 2008]: that the violence against civilians in Vietnam was not an aberration, but rather "pervasive and systemic," the inevitable and often intended result of US policies.

Among the most pernicious of these was the fanatical insistence on "body counts" as a measure of military success. The value of the tallies was not just symbolic: the more "kills" a unit called in, the better its position in the field. Trigger-shy troops were punished with "less support in the form of airlifts—resulting in long, hot, dangerous hikes through treacherous terrain instead of helicopter rides to or from the base," according to Turse, who shows due sympathy for the youthfulness (and fearfulness) of the GIs.

These vile incentives stemmed from the same systemic racism and strategic inconsistencies that doomed the American enterprise from the start. After learning in training that the "enemy is anything with slant eyes who lives in the village," US troops massacred the very South Vietnamese civilians for whom they were purportedly fighting. Turse only hints at how this tactical and moral perversity led directly to defeat.

The great contradiction of the war, and another lesson of this book, is that even as the United States officially downplayed the popularity of the Viet Cong insurgency, many US soldiers used it as a rationalization for slaughtering individual Vietnamese and even entire villages. A few common adages, quoted by Turse, bear this out: "If it's dead and Vietnamese, it's VC." "Kill 'em all and let God sort 'em out." "The sooner *they* all die, the sooner *we* go back to the World." And when civilians were "accidentally" killed? One marine explains: "No problem, just stick a chicom [Chinese communist] grenade on 'em, or an AK[-47], they become VC." Another, defending the murder of children: "Tough shit, they grow up to be VC." So why *were* we in Vietnam?

The real story of what the Vietnamese rightfully call "the American War" is not so much unknown as insufficiently recognized, less "untold" than too seldom acknowledged. In 1988, the late Alexander Cockburn wrote in this magazine that "My Lai remains a symbol, just an intimation of what happened in that destroyed land." Despite intensive (and ongoing) efforts to suppress that horrible reality—much of this book relies on files from the Vietnam War Crimes Working Group, a secret Pentagon project to investigate allegations of American atrocities, only to hide them from the public—it is Turse's immense achievement to have written a book that painstakingly chronicles at least a fraction of the murders and gang rapes committed in our name.

"We make more VC than we kill by the way these people are treated," one marine wrote to his parents, foreshadowing the absurdity of more recent US adventures. "I won't go into detail but some of the things that take place would make you ashamed of good old America." *Kill Anything That Moves*—words that appeared repeatedly in military directives during the war—makes it clear that if an American president ever did have the courage to embark on an "apology tour," Vietnam would have to be the first stop. ■

Richard Kreitner is a former Nation *intern.*

A Defense of Bulk Surveillance.

Authors: HERMAN, ARTHUR
YOO, JOHN[1]

Source: National Review. 4/7/2014, Vol. 65 Issue 6, p31-33. 3p.

Document Type: Article

Subject Terms: *MASS surveillance
*ELECTRONIC surveillance -- United States
*NATIONAL security -- United States
*RIGHT of privacy

Company/Entity: UNITED States. National Security Agency
UNITED States. Constitution. 4th Amendment

NAICS/Industry Codes: 928110 National Security

People: SNOWDEN, Edward Joseph, 1983-

Abstract: The article looks at the electronic surveillance carried out by the U.S. National Security Agency (NSA), as of 2014. The authors present a case for the view that the NSA's mass surveillance of phone call and e-mail records contributes to national security and does not overly intrude on Americans' privacy rights. Topics include the information disclosures of former NSA contract employee Edward Snowden and the U.S. Constitution's Fourth Amendment regarding search and seizure.

Author Affiliations: [1]law professor, University of California, Berkeley

ISSN: 0028-0038

Accession Number: 95006065

A Defense of Bulk Surveillance

The NSA programs enhance security without uniquely compromising privacy

BY ARTHUR HERMAN & JOHN YOO

At this writing, President Obama is set imminently to make one of the most momentous choices in the history of American intelligence. He will decide whether to curtail or terminate the National Security Agency's bulk collection of phone-call records and e-mail traffic in its quest to find and stop terrorist plots against the United States. President Obama could continue a program that takes advantage of America's technological superiority, meets the requirements of constitutional law, and has proven effective in stopping terrorist attacks. But, manipulated by intelligence leaks and stampeded by the demands of his anti-war base, he is likely to sacrifice national security in response to spurious claims of lost civil liberties.

In the wake of the September 11, 2001, terrorist attacks, the NSA established a program to trace phone calls and e-mails into the United States from suspected terrorists abroad. (One of us, John Yoo, judged the program to be constitutional as an official in the Justice Department in the months after the attacks.) The NSA already intercepts electronic communications abroad between foreigners in order to detect threats to U.S. national security and advance our foreign policy; that was the very purpose behind the establishment of the agency during the Cold War. To keep the intelligence agencies out of operations at home, however, the Foreign Intelligence Surveillance Act (FISA) allows only the FBI to eavesdrop on counterespionage and counterterrorism targets within the United States, after obtaining a special warrant.

The 9/11 attacks revealed a gap in this framework: The government had weakened its abilities to trace suspected terrorist calls and e-mails entering the U.S. by erecting a wall between the domestic and foreign aspects of electronic surveillance. Domestic- and foreign-intelligence officials could not share information or seamlessly monitor communications coming into, or passing through, the United States from abroad. In response, the NSA began collecting phone-call and e-mail records—their addressing information, rather than their content—to analyze patterns that might emerge once they were linked to a suspected terrorist message from abroad. The current head of the NSA, General Keith B. Alexander, has testified before Congress that the collection program has helped stop developing terrorist plots, and that had it existed in 2001, it could have led to the discovery of the 9/11 conspiracy.

Nevertheless, President Obama is now considering whether to end NSA surveillance as we know it. Even the most modest of his policy options—placing the database of call and e-mail records in the hands of private companies—would represent a radical change in the NSA's effectiveness, without much gain for privacy. A White House blue-ribbon panel has even proposed to end special national-security surveillance abroad by requiring a warrant, as is the case with domestic searches, and some in Congress want to end the NSA altogether.

This uncertainty is thanks to one man's success in generating international hysteria: Edward Snowden. Snowden apparently used his access as an NSA network administrator to steal massive amounts of U.S. military and intelligence secrets. Since fleeing to Hong Kong last June with four laptops jammed with classified data, Snowden has set up shop in Russia and has launched carefully stage-managed leaks of more and more secrets, such as U.S. surveillance of the telephones of foreign leaders. Snowden could not have done more damage to our national-security apparatus if he had been a Chinese or Russian mole.

Damage to the NSA doesn't arise just from the stolen technical data. It's also caused by the myths, misperceptions, and often downright lies about NSA data collection spread by Snowden and his supporters. Aided by a network of anti-government activists, Snowden has managed his leaks and distorted the truth to mislead the public into seeing the NSA data program as part of a vast Orwellian totalitarian nightmare, with our government gathering and inspecting the personal data of millions of innocent Americans.

Early on, for example, Snowden planted the notion that NSA workers were able to wiretap anyone, "even the president if I had a personal email," as he told the *Guardian* newspaper. We now know that this claim was completely untrue. Also flatly wrong was the notion that the NSA stores the content of phone calls—yet a recent poll revealed that 38 percent of Americans believe it *is* true. And the revelation that 80 percent of the phone calls about which the NSA collects data are made outside the United States has done nothing to decrease the impression that our smartphones and civil liberties are under daily assault.

As a result of Snowden's distorting leaks, the media routinely describe the NSA program as "domestic spying" or "eavesdropping." Even now, the American Civil Liberties Union website proclaims that "the government is regularly tracking almost every ordinary American and spying on a vast but unknown number of Americans' international calls, text messages, and emails."

While spreading conspiracy theories about a tyrannical "national-security state" has been standard left-wing practice since the 1960s, it is disappointing to see some on the right joining in. Even though a federal judge recently rebuffed the ACLU's lawsuit challenging the phone-data program, Senator Rand Paul (R., Ky.) is still suing the administration on the

Mr. Herman is the author of, among other books, Freedom's Forge: How American Business Produced Victory in World War II. *Mr. Yoo, a law professor at the University of California, Berkeley, and a visiting scholar at the American Enterprise Institute, is the author of* Point of Attack: Preventive War, International Law, and Global Welfare, *forthcoming in April.*

same ground, with the help of the Tea Party–backed think tank FreedomWorks and former Republican Virginia attorney general Ken Cuccinelli, who claims the suit is needed "to vindicate the Fourth Amendment rights of every American who uses a phone."

Critics must return to earth and remember that the program was set up in 2001 in order to, as President Obama himself has acknowledged, "address a gap identified after 9/11" in tracing "the communications of terrorists so we could see who they may be in contact with." The answer was to analyze metadata on millions of phone records from telecommunications providers in order to learn the numbers dialed by known terrorists. Only if analysis linked a pattern of suspicious calls to a terrorist could the government seek a warrant to learn the identity or content of the communications. In fact, far from involving unprecedented access to individual phone records or (in the case of the PRISM e-mail-surveillance program, launched in 2007) e-mail addresses, the NSA program is simply one more variant on the data-analysis techniques used by commercial companies.

With an eleven-judge panel overseeing every step, NSA handles data with a lot more care and supervision than Facebook or Google. Out of the thousands of NSA employees, for example, the phone database is handled by 22 technicians, and far from being deathly secret, their operating procedure is transparent, even (compared with the metadata's possible uses) banal. Algorithms sift through mountains of phone calls, including overseas calls, matching phone numbers to numbers with known terrorist links. Only when the technician can show one of seven superiors "a reasonable, articulable suspicion" that the number could be linked to a terrorist network is he or she allowed to pull up the dates of calls made and received over five years, the other parties' phone numbers, and the durations of the calls—and nothing else. The analyst may not listen to any calls, or read any text messages or e-mails sent on that phone, without a court warrant. Only after the NSA confirms a terror link through other sources can it pass the investigation on to the FBI, which can then seek a warrant for a wiretap.

How many times does this "reasonable, articulable link" get made? In all of 2012 there were exactly 288 such findings. In twelve of those cases, the NSA found grounds to pass the case on to the FBI—and in three of those, the information helped to prevent an attack. If Snowden and his congressional and White House allies have their way, that last number will be a zero.

Considering the millions of phone numbers making billions of phone calls that year and every year, these levels of surveillance can hardly be considered a major intrusive system. But what about the program's constitutionality and alleged violation of the Fourth Amendment? The Fourth Amendment does not protect some vague and undefined right to privacy. Instead, it declares: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause." The Constitution protects only the privacy of the "person," the home, and "papers and effects," which are usually located in the home. It does not reach information or things that we voluntarily give up to the government or to third parties outside of the home or our persons. The Fourth Amendment also does not make such information absolutely immune—it is still subject to search if the government is acting reasonably or has a warrant. These basic principles allow the government to search through massive databases of call and e-mail records when doing so is a reasonable measure to protect the nation's security, which is its highest duty.

It may perhaps be time to reconceive the rules of search and seizure in light of new Internet technologies, but that is the responsibility of our elected representatives.

The most lucid critique of the constitutionality of this logic comes not from Senator Paul or the ACLU, but from Judge Richard Leon of the federal district court in Washington, D.C. In *Klayman v. Obama*, Judge Leon declared that the NSA's bulk collection of phone records violated the Fourth Amendment to the Constitution. Leon's decision encountered a major obstacle: a Supreme Court precedent directly on point, *Smith v. Maryland* (1979). In *Smith*, the Court held that the government did not need a warrant to use what is known as a pen register, a device that records dialed phone numbers. According to the justices, there was no constitutional right to conceal phone numbers because callers provide them to a third party—the phone company. When we reveal private information to a third party, we lose privacy rights over it.

Judge Leon could not rule that *Smith*'s logic does not include telephone metadata, since the calling records collected by the NSA are exactly the same as the phone numbers that were held to be unprotected in *Smith*. Judge Leon instead concluded that technology has changed so much that *Smith* is no longer good law. The "almost-Orwellian technology" that allows the government to collect, store, and analyze phone metadata is "unlike anything that could have been conceived in 1979" and, "at best, the stuff of science fiction," Leon wrote. "I cannot imagine a more 'indiscriminate' and 'arbitrary invasion' than this systematic and high-tech collection and retention of personal data on virtually every single citizen for purposes of querying and analyzing it without prior judicial approval," he continued. "Surely, such a program infringes on 'that degree of privacy' that the founders enshrined in the Fourth Amendment."

Whether changed circumstances render *Smith v. Maryland* infirm was not for Judge Leon to decide. It may perhaps be

time to reconceive the rules of search and seizure in light of new Internet technologies, but that is the responsibility of our elected representatives. Only they can accountably determine what society's "reasonable expectation of privacy" is in Internet and telephone communications, balancing existing privacy rights against the government's need for information to protect the nation from terrorist attack. Judges are far too insulated and lack the expertise to make effective judgments on national security and foreign affairs.

If it comes to a judicial decision, the Supreme Court should find Judge Leon mistaken (as did a New York City federal district judge the following month). While the Fourth Amendment protects certain personal information, its text says nothing about the government's ability to analyze data that legitimately come into its hands. Under Judge Leon's theory, New York City's use of data-mining to predict high-crime spots would violate the Constitution, even though the information comes from public records of arrests and incidents that have happened in the past. In fact, if Judge Leon is right that the increase in the government's ability to collect and analyze information should suddenly confer on some data shared with third parties the constitutional protections now reserved for "persons, houses, papers, and effects," then the courts should protect all kinds of information besides what the NSA collects. Under his theory, the Fourth Amendment should also protect all credit-card information, financial transactions, travel reservations, and public Facebook and LinkedIn posts because the information, though no longer private, can be analyzed to make inferences about our activities. But, contrary to this argument, we have always allowed law-enforcement and national-security agencies to search information that has been handed over to private third parties.

Still, can we trust the NSA to stay within its limits and handle only phone-call and e-mail records? Critics point to one of Edward Snowden's earliest (and most misleading) leaks as proof that Americans aren't safe: a 2012 internal report that the program had crossed the line on privacy rules more than 2,776 times between April 2011 and March 2012. Taken out of context, that figure is utterly misleading: It is a tiny fraction of the billions of calls the NSA intercepts every year. The same report showed that more than two out of every three mistakes involved foreign targets living abroad, not Americans, and the vast majority were due to human error. One NSA employee, for example, typed "202," Washington's area code, instead of "20," Egypt's international code, on a database query.

These are hardly East German Stasi surveillance standards. They pale even beside the tools used by social-media companies to collect and analyze information about our buying, reading, and travel habits. The president did the men and women in our intelligence agencies a disservice when he suggested in a January speech that the program could lead to Stasi-style abuses. Interfering with these arrangements would greatly disrupt our anti-terrorism efforts while yielding no gain in individual privacy. President Obama could do no better than to allow the men and women on the front lines of America's intelligence wars to do their jobs and continue preventing terrorist attacks on the United States, which they have been doing against the odds for the last 13 years. NR

Welcome, Gentry

Development and affordable housing go together

BY REIHAN SALAM

A short while ago, Spike Lee, the celebrated African-American filmmaker, gave a wide-ranging lecture at Brooklyn's Pratt Institute. Among other things, he discussed the ongoing transformation of Brooklyn neighborhoods such as Fort Greene, where he was raised. At one point, he was asked whether there was an upside to "gentrification," in which more-affluent residents settle in neighborhoods that once were the preserve of low-income households, and he offered a spirited reply. Lee granted that gentrifying neighborhoods have better schools and police protection than they did in earlier eras. Yet he attributed the improvement in local public services to a kind of racism.

Neighborhoods like the South Bronx, Harlem, and Bedford–Stuyvesant had been plagued by low-quality services when he was young ("the garbage wasn't picked up . . . the police weren't around"), Lee recalled. But then, in Lee's imaginative retelling of recent New York City history, the influx of white residents suddenly led city officials to get their act together. Picture police officers taking naps as black people get mugged, then suddenly springing to life as white Park Slope moms start scolding them. Lee seemed to have forgotten that right-thinking liberals have been attacking the NYPD for being *over*zealous in poor black neighborhoods since at least the Giuliani years, not *under*zealous.

"So, why did it take this great influx of white people to get the schools better?" Lee asked. "Why's there more police protection in Bed–Stuy and Harlem now? Why's the garbage getting picked up more regularly? We been here!"

Like Spike Lee, I grew up in Brooklyn. I've been here too! And like Lee, I miss certain things about the Brooklyn of my childhood. Brooklyn wasn't cool or artisanal when I was a kid. It was rather dangerous, in fact. But I loved it because it was mine, and I share Lee's sense that some of Brooklyn's new arrivals don't seem to appreciate the qualities that make our hometown great.

That said, there are many things wrong with Lee's anti-gentrification soliloquy. Gentrification is not the product of a racist conspiracy. If it were, you'd think the racists responsible for improved police protection and garbage pick-up would notice that Bed–Stuy and Harlem still have large black majorities. Rather, gentrification is an opportunity, for New York City and for other cities that are home to strong local economies and high-poverty neighborhoods. Capitalizing on this opportunity is easier said than done. But if gentrification is handled the right way, it can benefit poor families striving to get ahead just as much as it benefits gentrifiers.

Real NSA Reform Still Needed.

Authors: COLE, DAVID (AUTHOR)

Source: Nation. 2/10/2014, Vol. 298 Issue 6, p3-4. 2p.

Document Type: Opinion

Subject Terms: *MASS surveillance
*ELECTRONIC surveillance -- United States
*CIVIL rights -- United States
*RIGHT of privacy

Company/Entity: UNITED States. National Security Agency

People: SNOWDEN, Edward Joseph, 1983-
OBAMA, Barack, 1961-

Abstract: The author looks at the debate over the mass electronic surveillance program of the U.S. National Security Agency (NSA) and its implications with respect to privacy and civil liberties, as of January 2014. Topics include the leaking of information about the NSA's activities by former NSA contract employee Edward Snowden and the reforms proposed by U.S. President Barack Obama, which the author says are inadequate.

ISSN: 0027-8378

Accession Number: 93934201

The Nation.
since 1865

Real NSA Reform Still Needed

Somewhere in Russia, Edward Snowden is smiling. On January 17, about eight months after Snowden's initial disclosures of National Security Agency spying run amok, President Obama gave a major speech in which he acknowledged the risks to privacy the NSA's activities pose and announced changes designed to limit those risks. The changes do not go nearly far enough, so Snowden's smile may be tempered. But none of these changes would have happened had it not been for the leaks.

So long as the NSA programs remained secret, Obama maintained them, the federal courts blessed them and Congress authorized them (albeit unwittingly for most members). Now that the programs have been exposed, Obama has promised to rein them in, the courts have begun to question their constitutionality and Congress is considering a slew of bills to reform them. Funny how transparency works.

Snowden can't take all the credit, of course. Organizations dedicated to protecting privacy, including the ACLU, the Electronic Privacy Information Center, the Electronic Frontier Foundation and the Center for Democracy and Technology all played outsize roles, before and after Snowden's leaks, underscoring the importance of privacy and the risks that new technologies pose. And of course the press, including *The Guardian*, *The Washington Post* and *The New York Times*, along with journalists Glenn Greenwald and Barton Gellman, have used Snowden's documents to expose and explain what the agency has been doing. Americans from the right and the left have voiced concerns, which have been amplified in turn by the rest of the world—not surprising, as the vast majority of the NSA's targets are foreign nationals.

But privacy advocates will have to keep pressing their cause if they want real reform. The changes Obama announced are only a first step. They are more than cosmetic, but they leave largely intact the system of dragnet surveillance the NSA piloted. True reform would replace that mass surveillance with a more targeted approach, one that authorizes intrusive surveillance when the agency has reason to suspect a person of wrongdoing or of being a foreign agent, but not otherwise.

Obama sees the problem but is unwilling, or unable, to provide an adequate solution. He admitted that the digital age presents profound challenges to privacy: "The power of new technologies means that there are fewer and fewer technical constraints on what we *can* do. That places a special obligation on us to ask tough questions about what we *should* do."

And Obama pointedly rejected the argument that if phone companies and Internet service providers have our digital information, there is no reason the government shouldn't also have it. This is the argument the Supreme Court accepted in 1979 in *Smith v. Maryland*, when it ruled that the government could obtain a person's phone calling records without constitutional limits. Obama rightly insisted that there is a big difference between Verizon knowing that information and the government knowing it: "All of us understand that the standards for government surveillance must be higher. Given the unique power of the state, it is not enough for leaders to say: trust us, we won't abuse the data we collect."

Obama called for closer judicial oversight of NSA searches of telephone metadata; for a panel of independent lawyers to defend privacy before the secret foreign intelligence court; and for extending some privacy protections enjoyed by US citizens to foreign nationals. But his reforms leave in place the NSA's bulk collection of telephone

VOLUME 298, NUMBER 6, February 10, 2014

The digital version of this issue is available to all subscribers January 23 at TheNation.com.

Cover: photographed by Francis Reynolds, styled by Dan Reisman

BY THE NUMBERS

33%
Reduction in West Virginia's rate of uninsured because of Medicaid expansion

$20M
Estimated amount spent by Americans for Prosperity on its anti-Obamacare ad buy

8.05X
Rate at which blacks are more likely to be arrested than whites for marijuana possession in Washington, DC

"I smoked pot as a kid, and I view it as a bad habit and a vice, not very different from the cigarettes that I smoked.... I don't think it is more dangerous than alcohol."

President Obama, in an interview with *The New Yorker*'s David Remnick

data from every American's every phone call, as well as its sweeping authority to intercept electronic communications of people it believes to be foreigners abroad without any basis for suspecting them of wrongdoing. And Obama did not even mention—much less suggest an effort to rein in—the NSA's vacuuming up of massive amounts of data from Google and Yahoo communications hubs overseas, or its collection of massive amounts of cellphone-location data and e-mail address books, all without any statutory limits.

Obama sought to assure his listeners that the NSA would not spy on ordinary people doing nothing wrong. But that's false. The whole point of the programs he has left in place is to conduct dragnet surveillance of ordinary people engaged in no wrongdoing—in the hope that if the NSA casts its net wide enough, it may capture a terrorist.

So Obama acknowledged the problem—and for that, Snowden and privacy advocates deserve our thanks. But the president failed to solve it. Fortunately, it seems no one was fooled. The speech received a cool reception from most overseas and US commentators, and a *USA Today* poll reports a majority disapproves of the NSA programs. The debate will continue. Congress is considering dozens of bills that would go further, and several legal challenges are pending in the courts. If we are to preserve privacy in the digital age, we must insist that Obama's speech be understood as the beginning, not the end, of NSA reform. DAVID COLE

David Cole is The Nation's *legal affairs correspondent.*

Amnesty for Snowden!

Justice demands full exoneration.

COMMENT

How we adore the whistleblowers of the past! Daniel Ellsberg is now a national treasure and walking civics lesson for leaking the Pentagon Papers—the State Department even screens a documentary about him abroad as an advertisement for the American way. And behold the glowing coverage *The New York Times* has given the antiwar activists who in 1971 broke into an FBI office in Media, Pennsylvania, stole nearly 1,000 documents, and exposed the bureau's illegal and rampant political spying. The *Times* portrayed the FBI burglars as exemplary citizens.

But the whistleblowers of the present are another matter—and always have been. At the height of the Pentagon Papers uproar, Ellsberg never enjoyed as much popular support as Lt. William Calley, a Vietnam war criminal later pardoned by President Nixon. White House aide John Ehrlichman suggested that Ellsberg was a Soviet spy—sound familiar? (In the end, Ellsberg beat the criminal charges against him only because the sloppy thugs of Team Nixon broke the law so wantonly in pursuit of him.) And when the Media burglars sent copies of the FBI's political files to the *Times*, the journal of record immediately handed the documents over to the FBI. So did the Senate office of George McGovern. It can take decades for whistleblowers to be canonized.

All of which makes the surging support for Edward Snowden remarkable. Despite official scaremongering, Americans are alarmed by intrusive state surveillance. And despite news coverage that has not always been distinguishable from an NSA press release—for instance, December's cringeworthy *60 Minutes* segment anchored by a career PR flack for various police and security bureaucracies—a huge majority of Americans, according to a recent *USA Today*/Pew Research poll, oppose the NSA's phone metadata collection. What's more, a plurality think Snowden's leaks were good for the country, even if he did break the law.

But the law is the law, as countless commentators displeased with Snowden have reminded us. Funny, those talking sternly of the law's impartial majesty tend not to call for the indictment of intelligence czar James Clapper, despite his false-on-their-face statements to Congress—a federal felony. Instead, we are treated to jesuitical distinctions between Snowden and Ellsberg and the Media burglars, who were in their time accused of jeopardizing national security. Meanwhile (if anyone cares to listen), Ellsberg and the Media burglars have voiced their unqualified support for Snowden and his profoundly moral disclosures.

Snowden's leaks are not just about moral principle, however. They will likely alter how we are governed. The impact is not instantaneous—after all, the revelations about J. Edgar Hoover's COINTELPRO octopus took years to result in legislation that leashed the FBI and CIA to the Constitution. Already, Snowden's leaks are propelling good legislative action. Last July, a House vote to eliminate funding for the NSA's phone surveillance programs lost by only twelve votes, with a majority of Democrats opposing the president. There will be more such battles, and they will fracture both parties into civil libertarian and authoritarian wings, scrambling the conventional political spectrum in a most clarifying way. Some Democrats are uncomfortable criticizing their president, while others seem alarmingly comfortable defending him. Civil libertarians of both parties need to work together—and not just on the matter of Snowden—since a strong inter-party alliance is the only thing that can protect our freedoms from the increasingly predatory behavior of American law enforcement.

The reforms announced by President Obama are a welcome start, but they should be a floor, not the ceiling, to systemic changes in our bloated, intrusive and unaccountable security apparatus. But there is one response to these revelations that remains essential. Every legal system in the world has some form of clem-

The AP's Privacy, and Ours.

Authors: COLE, DAVID (AUTHOR)

Source: Nation. 6/10/2013 Double Issue, Vol. 296 Issue 24/25, p4-6. 3p.

Document Type: Opinion

Subject Terms: *GOVERNMENTAL investigations -- United States
*LEAKS (Disclosure of information)
*RIGHT of privacy
*SEARCHES & seizures (Law)
*TELECOMMUNICATIONS laws & regulations
UNITED States

Company/Entity: UNITED States. Dept. of Justice
ASSOCIATED Press -- Officials & employees

Abstract: The article comments on the U.S. Department of Justice's (DOJ's) obtaining the phone records of Associated Press news agency reporters without court approval to determine who leaked information about the Central Intelligence Agency's (CIA's) infiltration of a terrorist cell. The DOJ's action and privacy rights are discussed. The article notes cell phone records are not protected by the Fourth Amendment. It also notes the Electronic Communications Privacy Act's (ECPA's) limitations.

ISSN: 0027-8378

Accession Number: 87770902

The Nation.

EDITOR & PUBLISHER: Katrina vanden Heuvel

PRESIDENT: Teresa Stack

MANAGING EDITOR: Roane Carey
LITERARY EDITOR: John Palattella
EXECUTIVE EDITORS: Betsy Reed, Richard Kim (*online*)
SENIOR EDITORS: Richard Lingeman, Emily Douglas (*online*)
COPY DIRECTOR: Rick Szykowny
COPY CHIEF: Judith Long
ASSOCIATE LITERARY EDITOR: Miriam Markowitz
ASSOCIATE EDITOR: Liliana Segura
ASSISTANT COPY EDITOR: Matthew Grace
COPY ASSOCIATE: Lisa Vandepaer
MULTIMEDIA EDITOR: Francis Reynolds
COMMUNITY EDITOR: Annie Shields
RESEARCH DIRECTOR/ASSISTANT EDITOR: Kate Murphy
ASSISTANT TO THE EDITOR: Barbara Stewart
INTERNS: Alleen Brown, James Cersonsky, Catherine Defontaine, Andrew Bard Epstein, Luis K. Feliz, Elana Leopold, Alec Luhn, Anna Simonton (*Washington*), Cos Tollerson, Sarah Woolf

WASHINGTON CORRESPONDENT: John Nichols; **REPORTER:** George Zornick

NATIONAL AFFAIRS CORRESPONDENT: William Greider

EDITOR AT LARGE: Christopher Hayes

COLUMNISTS: Eric Alterman, Melissa Harris-Perry, Naomi Klein, Katha Pollitt (*on leave*), Jessica Valenti, Patricia J. Williams, Gary Younge

DEPARTMENTS: *Architecture*, Michael Sorkin; *Art*, Barry Schwabsky; *Corporations*, Robert Sherrill; *Defense*, Michael T. Klare; *Environment*, Mark Hertsgaard; *Films*, Stuart Klawans; *Legal Affairs*, David Cole; *National Security*, Jeremy Scahill; *Net Movement*, Ari Melber; *Peace and Disarmament*, Jonathan Schell; *Poetry*, Jordan Davis; *Sex*, JoAnn Wypijewski; *Sports*, Dave Zirin; *United Nations*, Barbara Crossette; *Deadline Poet*, Calvin Trillin

CONTRIBUTING EDITORS: Kai Bird, Robert L. Borosage, Stephen F. Cohen, Marc Cooper, Arthur C. Danto, Mike Davis, Slavenka Drakulic, Robert Dreyfuss, Susan Faludi, Thomas Ferguson, Doug Henwood, Max Holland, Michael Moore, Christian Parenti, Richard Pollak, Joel Rogers, Karen Rothmyer, Robert Scheer, Herman Schwartz, Bruce Shapiro, Edward Sorel, Jessica Valenti, Jon Wiener, Amy Wilentz, Art Winslow

CONTRIBUTING WRITERS: Ben Adler, Ari Berman, William Deresiewicz, Lee Fang, Liza Featherstone, Laura Flanders, Dana Goldstein, Eyal Press, Lizzy Ratner, Scott Sherman, Wen Stephenson, Kai Wright

BUREAUS: *London*, Maria Margaronis, D.D. Guttenplan; *Southern Africa*, Mark Gevisser

EDITORIAL BOARD: Deepak Bhargava, Norman Birnbaum, Barbara Ehrenreich, Richard Falk, Frances FitzGerald, Eric Foner, Greg Grandin, Philip Green, Lani Guinier, Tom Hayden, Ilyse Hogue, Tony Kushner, Elinor Langer, Deborah W. Meier, Toni Morrison, Walter Mosley, Victor Navasky, Pedro Antonio Noguera, Richard Parker, Michael Pertschuk, Elizabeth Pochoda, Marcus G. Raskin, Kristina Rizga, Andrea Batista Schlesinger, Dorian T. Warren, David Weir, Roger Wilkins

ASSOCIATE PUBLISHER, SPECIAL PROJECTS/WEBSITE: Peter Rothberg
ASSOCIATE PUBLISHER/DEVELOPMENT: Peggy Randall
DIRECTOR OF FINANCE: Mary van Valkenburg
HUMAN RESOURCES DIRECTOR: Jeanne Perry
VICE PRESIDENT, ADVERTISING: Ellen Bollinger
ADVERTISING DIRECTOR: Amanda Hale
VICE PRESIDENT, CIRCULATION: Arthur Stupar
CIRCULATION MANAGER: Michelle O'Keefe
AUDIENCE DEVELOPMENT & DIGITAL MARKETING MANAGER: Katelyn Belyus
VICE PRESIDENT, PRODUCTION/MARKETING SERVICES: Omar Rubio
PRODUCER/WEB COPY EDITOR: Sandy McCroskey
PRODUCTION COORDINATOR: Mel Gray
DIRECTOR OF NATION BUILDERS/INVESTOR RELATIONS: Joliange Wright
NATION BUILDERS ASSISTANT/AD SALES PLANNER: Loren Lynch
PUBLICITY DIRECTOR: Caitlin Graf
CIRCULATION/BUSINESS ASSISTANT: Vivian Gómez
DIRECTOR, DIGITAL PRODUCTS: John W. Cary
DIGITAL PRODUCT MANAGER: Joshua Leeman
TECHNOLOGY MANAGER: Jason Brown
BOOKKEEPER: Maura MacCarthy
ASSISTANT TO VICTOR NAVASKY: Mary Taylor Schilling
DATA ENTRY/MAIL COORDINATOR: John Holtz
ASSISTANT TO THE PRESIDENT: Kathleen Thomas
COMMUNITY COORDINATOR/BUSINESS ASSISTANT: Sarah Arnold
ADVERTISING ASSISTANT: Kit Gross
ACADEMIC LIAISON: Charles Bittner

PUBLISHER EMERITUS: Victor Navasky

LETTERS TO THE EDITOR: E-mail to letters@thenation.com (300-word limit). Letters are subject to editing for reasons of space and clarity.

SUBMISSIONS: Queries only, no manuscripts. Go to TheNation.com and click on "about," then "submissions" for a query form. Poetry may be mailed to The Nation, 33 Irving Place, New York, NY 10003. SASE.

INTERNET: Selections from the current issue become available Thursday morning at TheNation.com.

Printed on 100% recycled 40% post-consumer acid- and chlorine-free paper, in the USA.

specific legislation to guarantee privacy rights for all. A bipartisan group of House members—libertarian Republicans and progressive Democrats—has proposed a Telephone Records Protection Act, which would require that the government obtain court approval to get telephone records from service providers. That's a baseline standard for protecting the privacy of every American, including the reporters, imperfect as they may be, who arm the citizenry with the power which knowledge gives.

The AP's Privacy, and Ours

On a Friday afternoon in May, a lawyer for the Associated Press received a letter from the Justice Department informing the news agency that, unbeknownst to it, the DoJ had obtained two months' worth of phone records for twenty AP phone lines—including the personal and office lines of five reporters and an editor—at several AP bureaus. The records were obtained without the approval of a court, and without advance notice to the AP or the affected journalists.

COMMENT

The press is, as expected, up in arms, as are members of Congress from both parties. But it's far from clear that the DoJ did anything wrong. Because the subpoena was issued in an ongoing criminal investigation, there is only limited public information about why the prosecutor made such a sweeping request. But the leak being investigated was indisputably serious. It concerned an ongoing CIA operation that had apparently infiltrated a terrorist cell of Al Qaeda in the Arabian Peninsula. Whoever revealed that fact was no whistleblower; it's difficult to see any possible justification for revealing that we had infiltrated a terrorist cell. The AP, at the government's request, did delay publishing the story, but that hardly exculpates the leaker, who compromised a critically important ongoing investigation. Attorney General Eric Holder called it one of the gravest leaks he's seen in his entire career.

The Justice Department sought the AP records only after spending months pursuing other avenues to identify the leaker, including interviewing 550 people. Only when the interviews proved fruitless did he seek the reporters' phone records. Five reporters and one editor worked on the story, and if there was no other way to narrow the inquiry, it's possible that the request for records was justified, and would have been authorized had the Justice Department sought court approval.

We know from past experience that there are legitimate grounds for concern about overclassification, punishment of whistleblowers and the chilling of press freedoms. But that doesn't mean that every leak is an act of heroism, or that every journalist should be immune from criminal investigation. Our legitimate concerns will lose credibility if we too often respond with a jerk of the knee.

But the specifics of the leak and subpoena are much less important than what the incident reveals about the law's failure to protect not just the press's confidential communications, but the privacy rights of us all in the digital age. Consider this: in 2011 alone, cellphone companies responded to 1.3 million sub-

poenas and other requests from law enforcement for subscriber information, including text messages, phone data and location information. Verizon alone responded to more than 260,000 requests. And the numbers have been increasing dramatically each year. AT&T received an average of 700 law enforcement requests a day in 2011, up by 300 percent from 2007.

Why the dramatic increase? So many of us carry smart phones, on which we record our transactions—phone calls, text messages, e-mails, Internet browsing and the like. Smart phones also transmit to our service providers a record of our physical whereabouts. This information can be highly useful to criminal investigations. It can refute an alibi, help identify co-conspirators, track fraudulent transactions and the like. But it can also disclose nearly everything about our personal lives that we do not keep stored exclusively in our (as yet) unwired brains.

Thanks to the Supreme Court, these records receive no Fourth Amendment protection when, as in the AP investigation, the government gets them from a third party, in this case the phone company. Long ago, the Court ruled that we have no "reasonable expectation of privacy" with respect to information we share with others, and therefore no protection against the government's obtaining that information from a third party. Because everything we do on our phones is "shared" with our service provider at a minimum, the Fourth Amendment requires no warrant or probable cause for the government to seek such information.

Since the Supreme Court has essentially bowed out, our protections depend on Congress, which has required, for example, that the government present specific facts to justify obtaining real-time phone records of whom we call and for how long. It requires the same for stored e-mail transmissions. But even that requirement—a standard less rigorous than probable cause—does not apply to stored records of phone transactions. That's why the DoJ could obtain the AP reporters' phone records (and ours) without a court order or a specific showing of need.

More disturbing still, if the government wants to read the content of our e-mails, not just the address information, the Electronic Communications Privacy Act (ECPA) requires it to obtain a warrant only if the e-mails are less than six months old; once they've been stored for more than six months, they lose that protection. At the time the law was enacted, e-mail storage space was limited, and it was thought that few e-mails would be stored that long. But with the advent of unlimited storage in the cloud, the norm today is to keep all but junk e-mail. Should the contents of our e-mails be available to government prying just because they are far down in our inbox?

In other words, the problem here is not one of press freedom. It's more fundamental: it's about privacy generally. The Fourth Amendment's protections are increasingly going the way of the land line and the cassette player, rendered obsolete by technological innovations. We are unlikely to give up carrying our homing devices, otherwise known as cellphones. Unless we insist on statutory protection, it's not just AP reporters but all of us who will be at the mercy of a prosecutor's discretion.

Senator Charles Schumer has revived a federal press shield

Noted.

REMEMBERING CYNTHIA BROWN: **Cynthia Brown** died peacefully in her Manhattan apartment on May 12, following a fierce two-year battle with cancer. She wrote her first story for *The Nation* in 1979, when as a brilliant 26-year-old journalist covering Latin America she reported on the irreparable damage done to **Nicaragua** by the Somoza regime.

Cynthia led the way for a generation of independent journalists and filmmakers—including **Susan Meiselas, Anne Nelson, Julia Preston** and **Pamela Yates**, among others—who approached the coverage of events in this hemisphere through the lens of human rights. Their reporting departed strikingly from the normative framing of the Cold War years, in which the inability to see past the threat of communism—as well as to recognize the legitimate aspirations of regional populations to self-determination and democracy—repeatedly led the United States into ill-advised alliances with military dictatorships and politically repressive regimes.

Cynthia and her contemporaries reframed our understanding of these issues and our role in the hemisphere, and their reporting inspired efforts in Congress to blunt the interventionist doctrine of the Reagan era. In the pages of *The Nation*, Cynthia documented the ravages of US-supported dictatorships in **El Salvador, Guatemala, Uruguay** and especially **Chile**, the country that claimed her heart.

She worked for seventeen years at **Human Rights Watch**, first as a researcher for **Americas Watch**, later as the Americas Watch representative in Chile, and then as the organization's first program director. Principled and uncompromising, committed to the facts and to analytical rigor, she placed her distinctive mark on the emerging human rights standards by which the performance of governments throughout the world came to be measured.

Cynthia died way too young, but not before making a huge difference in the times in which she lived. HAMILTON FISH

VACATION FROM WAR: Once again it's time to honor an annual tradition and donate to **Vacation From War.** This German-based peace group is celebrating its twentieth year of bringing together children for a multiethnic summer camp in the wake of civil war. Today it includes children from **Croatia** and **Serbia**, Albanians and Serbs from **Kosovo**, and young people from **Israel** and occupied **Palestine.** *Nation* readers are a mainstay of the organization, so please open your hearts and wallets: $150 makes you a godparent, but donations of any size are welcome.

Make out your checks to "Vacation From War," mail them to me at *The Nation* (33 Irving Place, New York, NY 10003), and I will forward them. KATHA POLLITT

HELP OKLAHOMA: Oklahoma's most impoverished residents were hit hard by the tornado that struck on May 20, and support is critically needed. Among the best groups to donate to are the **Oklahoma Tornado Relief Fund**, the **Regional Food Bank of Oklahoma**, **Feeding America** and **Operation: Starting Gun.** For more background on their work, visit TheNation.com. PETER ROTHBERG

law, but that's not sufficient. The problem goes much further. Four members of Congress (Republicans Justin Amash and Mick Mulvaney, and Democrats Zoe Lofgren and Jared Polis) have introduced a bill to require court orders for access to phone records—not just for the AP or other members of the press, but for us all. And last year a Senate committee approved amendments to the ECPA that would protect the contents of all e-mails, eliminating the outmoded six-month time limitation. These legislative reforms, and others, are critical if we are to preserve privacy in an age when law enforcement officials make more than 1.3 million requests a year to our communications service providers for our most private information. DAVID COLE

David Cole is The Nation*'s legal affairs correspondent.*

No More Rana Plazas

We mark the one-month anniversary of the horrific Rana Plaza disaster, the collapse of an eight-story building in a suburb of Dhaka, Bangladesh, which killed more than 1,110 garment workers. Rana Plaza has proved to be a watershed moment, galvanizing a global call to action to clean up the fashion industry. But it has also revealed a major roadblock to reform: fashion brands aren't held responsible for what happens in the factories that make their products, and American clothiers are merely giving lip service to tougher standards.

COMMENT

Here's where we are: more than a dozen major European fashion brands—including H&M, Tesco, Primark, Benetton and Mango—have signed on to Accord on Fire and Building Safety in Bangladesh, a legally binding, landmark agreement that requires brands to make their suppliers in Bangladesh submit to independent inspections, make the results of those inspections public and help fund any necessary improvements to building safety. Dishearteningly and embarrassingly, the vast majority of US retailers—including Walmart, Gap, J.C. Penney, Sears, Kohl's, Target and Macy's—have not signed on.

Walmart, one of the largest buyers of clothing from Bangladesh, has decided to inspect its suppliers itself. The suggestion that Walmart is capable of monitoring its own supply chain is particularly appalling, given that it is linked to the Tazreen factory fire, which killed 112 Bangladeshi workers in November, and also sold jeans from a supplier that placed an order in Rana Plaza.

President Obama has been eerily silent on the issue, though there is much he could do. If Obama is unsure of how to act, he might start where former President Bill Clinton left off in 1996. Following a string of sweatshop scandals (including the infamous case of Walmart's Kathie Lee Gifford brand, whose products were found to be made by children in Honduras), Clinton established a presidential task force on apparel made up of labor leaders, human rights and religious groups, and reps from companies like Nike and L.L. Bean. Aside from improving the factories, the task force's goal was to give Americans a way to track the conditions under which their clothing was made.

The outcome of Clinton's White House Apparel Industry Partnership was to establish a baseline standard for working conditions in garment factories around the world (it set workweek hours at sixty, for example, and banned child labor). But those standards didn't go far enough (a living wage should be the new goal), and they aren't enforceable. The task force also set up an auditing group, the Fair Labor Association, to inspect progress in factories and make the results of its inspections public. Monitoring alone leaves garment workers vulnerable because it's voluntary, and brands often use marginal improvements in their supply chain as success stories for branding purposes. Last year, for example, the FLA came under sharp criticism when it claimed that working conditions at Apple's notorious Foxconn factory showed "continued improvements." The AFL-CIO called social auditing firms, including the FLA, a "facade."

In the past fifteen years, the apparel industry, and the world, have undergone seismic changes, for which Obama's twenty-first-century apparel task force would have to account. Clothing imports to the United States have skyrocketed since 1996 (we now manufacture only 3 percent of our clothing), which makes monitoring conditions that much more difficult—and crucial. But this is an opportunity for real change here and abroad: lifting wages and conditions for garment workers worldwide will benefit workers in places like Bangladesh as well as give our country's garment and textile manufacturers a chance to compete. The government of Bangladesh recently announced it would increase the minimum wage and allow garment workers to form unions without the approval of their employers. These are promising developments; wage increases and the right to unionize must be realized and protected.

We also need the leadership of our first lady, a fashion icon who shops at H&M and Target, which produce clothes in Bangladesh. She must help change the culture of fashion in the United States. Ultra-cheap consumer goods contribute directly to our economic woes and are linked to human tragedy abroad, yet Americans celebrate bargain fashion and have stockpiled our closets with gobs of disposable trends. Fairly and affordably priced fashion should be our new goal—and, obviously, fashion should never come at the cost of lives. Michelle Obama would be the perfect spokesperson for such a message.

The Clinton-era task force was a good start, but the new presidential task force should fulfill the promise that people be able to

Calvin Trillin, Deadline Poet

Another Week in the White House

The IRS has made a mess
That brings the White House many stresses.
They need distractions, which they've got—
Alas, though, those are other messes.

Advertisements Starring ... You.

Authors: Rayman, Noah

Source: Time. 10/28/2013, Vol. 182 Issue 18, p16. 1p. 1 Color Photograph.

Document Type: Article

Subject Terms: *INTERNET advertising
*INTERNET users -- Legal status, laws, etc.
*RIGHT of privacy -- Lawsuits & claims
*ADVERTISING campaigns
SOCIAL aspects
ECONOMIC aspects

Company/Entity: GOOGLE Inc. -- Management

Reviews & Products: FACEBOOK (Web resource) -- Social aspects
TWITTER (Web resource) -- Social aspects

NAICS Industry Codes: 541870 Advertising Material Distribution Services

Abstract: The article discusses Internet advertising campaigns involving users of social media networks and Internet companies such as Google Inc. in the U.S. as of October 2013, focusing on the social networking service Facebook and privacy-related lawsuits by Internet users. According to the article, the social-ad business may be worth over nine billion dollars in sales in the U.S. in 2013. The Twitter social networking company is mentioned, along with the Instagram photo-sharing service.

Full Text Word Count: 391

ISSN: 0040-781X

Accession Number: 91279934

Publisher Logo:

TIME

Advertisements Starring ... You

Listen American Accent

Popular sites are trying to cash in on users' connections

Your friends may be the most effective pitchmen. In the latest sign that technology firms are increasingly deploying users' data to boost ads, Google announced on Oct. 11 that it was changing its terms of service to allow the company to combine users' posts, reviews and profile photos in advertisements beginning next month. Here's how it works: a user searching Google for, say, a date-night restaurant might see text ads promoting a local eatery--along with a friend's face and review on the firm's social network, Google+. A whopping 87% of the search giant's $50 billion in annual revenue comes from advertising, and Google is betting this information will make ads clickier.

Rival Facebook has already found that pitching products with a friend's endorsement--a Like or positive post--makes for more-powerful ads, which accounted for most of the social network's $5 billion in revenue last year. Research firm eMarketer estimates that the so-called social-ad business will be worth $9.5 billion in U.S. sales this year. But it can be a risky business. In August, a judge approved Facebook's settlement of a class-action suit over employing users in ads, and the company agreed to give them control over when they're drafted to promote a product. "They're still walking a tightrope," explains consultant Jake Wengroff of firms trying such ads. The practice, he says, can alienate users and open companies to privacy suits. Still, given the potential profits in better ads, analysts say it might be a risk worth taking. Here's a look at what companies are trying.

TWITTER

Brands can pay to have users' tweets amplified across the site--with permission. Retweets essentially become easy marketing.

GOOGLE

Google's new ads won't show up only in search; they could also one day appear across services such as e-mail and maps. Users can opt out.

FACEBOOK

Users' Likes and photos can appear in ads targeted to their friends. Users can opt out.

INSTAGRAM

Facebook's photo-sharing site says it plans to launch ads in the next few months. It backtracked last year on a policy that would have given advertisers access to users' photos.

PINTEREST

The content-sharing site hasn't said whether it will incorporate users' connections into the ads it recently rolled out.

PHOTO (COLOR)

~~~~~~~~

By Noah Rayman
~~~~~~~~