INTERNET TRACKING

NICHOLAS CARR

Nicholas Carr was born in 1959 and educated at Dartmouth College and Harvard University. He worked as a management consultant for a private firm and as executive editor for *Harvard Business Review* and is currently an editorial advisor for *Encyclopaedia Britannica*. Carr is best known, however, for his worrisome insights into computers and culture. He stirred controversy with his first two books, both skeptical of the benefits of technology for business: *Does IT Matter? Information Technology and the Corrosion of Competitive Advantage* (2004) and *The Big Switch: Rewiring the World, from Edison to Google* (2008). His most recent book, *The Shallows: What the Internet Is Doing to Our Brains* (2011), examines how constant connectedness is harming people and was a finalist for the Pulitzer Prize for general nonfiction. Carr's writing has also appeared in several newspapers and magazines, including *The Atlantic Monthly*, *Financial Times*, *Wired*, the *New York Times*, and *Advertising Age*. He is a sought-after speaker on the business lecture circuit and a regular commentator on television and radio.

Tracking Is an Assault on Liberty

Carr is a leading skeptic about the benefits of the Internet and often writes about the dangers of spending time online. In this 2010 essay for the *Wall Street Journal*, he cites examples of how corporations collect and use our personal information online, warns of potential abuses of such data mining, and advocates new rules protecting consumer privacy. The essays following this one — Jim Harper's "Web Users Get as Much as They Give" (p. 545) and Lori Andrews's "*Facebook* Is Using You" (p. 551) — address the same issue.

In a 1963 Supreme Court opinion, Chief Justice Earl Warren observed that "the fantastic advances in the field of electronic communication constitute a great danger to the privacy of the individual." The advances have only accelerated since then, along with the dangers. Today, as companies strive to personalize the services and advertisements they provide over the Internet, the surreptitious collection of personal information is rampant. The very idea of privacy is under threat. 1

Most of us view personalization and privacy as desirable things, and we understand that enjoying more of one means giving up some of the other. To have goods, services and promotions tailored to our personal circumstances 2

and desires, we need to d
governments or other out
This tradeoff has alw
But now, thanks to the N
those tradeoffs — to chc
quences, what informati
Incredibly detailed data
bases without our awarei

Even though the In
seclusion. We often assu
online. As a result, we t
but as a personal diary
visit and the searches
hobbies, families, polit
even our peccadilloes.

But our sense of ar
we do online, down t
in cookies and corpor
explicitly through our
assigned to our comp
purchasing histories.

A few years ago.
results of an experime
extract sensitive pers
of software that allow
customers post to cat
receive as gifts. These
or her city and state.

Using a couple
over 250,000 wish li
controversial or poli
Slaughterhouse-Five[1]
tify addresses and pl

Mr. Owad ende
of people interestec
Nineteen Eighty-Fo

[1] A 1969 novel ab
in World War II. — E

[2] A 1949 novel c
writing, see p. 619.) —

G

tmouth College and Har-
ant for a private firm and
l is currently an editorial
vn, however, for his worri-
controversy with his first
gy for business: *Does IT*
of Competitive Advan-
d, from Edison to Google
e Internet Is Doing to Our
ss is harming people and
fiction. Carr's writing has
s, including *The Atlantic*
, and *Advertising Age*. He
: and a regular commenta-

Liberty

net and often writes about
y for the *Wall Street Jour-*
ld use our personal infor-
a mining, and advocates
following this one — Jim
545) and Lori Andrews's
issue.

ice Earl Warren observed 1
ic communication consti-
" The advances have only
lay, as companies strive to
rovide over the Internet,
is rampant. The very idea

desirable things, and we 2
up some of the other. To
ir personal circumstances

and desires, we need to divulge information about ourselves to corporations, governments or other outsiders.

3 This tradeoff has always been part of our lives as consumers and citizens. But now, thanks to the Net, we're losing our ability to understand and control those tradeoffs — to choose, consciously and with awareness of the consequences, what information about ourselves we disclose and what we don't. Incredibly detailed data about our lives are being harvested from online databases without our awareness, much less our approval.

4 Even though the Internet is a very social place, we tend to access it in seclusion. We often assume that we're anonymous as we go about our business online. As a result, we treat the Net not just as a shopping mall and a library but as a personal diary and, sometimes, a confessional. Through the sites we visit and the searches we make, we disclose details not only about our jobs, hobbies, families, politics and health, but also about our secrets, fantasies, even our peccadilloes.

5 But our sense of anonymity is largely an illusion. Pretty much everything we do online, down to individual keystrokes and clicks, is recorded, stored in cookies and corporate databases, and connected to our identities, either explicitly through our user names, credit-card numbers and the IP addresses assigned to our computers, or implicitly through our searching, surfing and purchasing histories.

6 A few years ago, the computer consultant Tom Owad published the results of an experiment that provided a chilling lesson in just how easy it is to extract sensitive personal data from the Net. Mr. Owad wrote a simple piece of software that allowed him to download public wish lists that *Amazon.com* customers post to catalog products that they plan to purchase or would like to receive as gifts. These lists usually include the name of the list's owner and his or her city and state.

7 Using a couple of standard-issue PCs, Mr. Owad was able to download over 250,000 wish lists over the course of a day. He then searched the data for controversial or politically sensitive books and authors, from Kurt Vonnegut's *Slaughterhouse-Five*[1] to the Koran. He then used *Yahoo!* People Search to identify addresses and phone numbers for many of the list owners.

8 Mr. Owad ended up with maps of the United States showing the locations of people interested in particular books and ideas, including George Orwell's *Nineteen Eighty-Four*.[2] He could just as easily have published a map showing

[1] A 1969 novel about alien abduction, time travel, and the bombing of Dresden, Germany, in World War II. — EDS.

[2] A 1949 novel critical of communism and mind control. (For an example of Orwell's writing, see p. 619.) — EDS.

the residences of people interested in books about treating depression or adopting a child. "It used to be," Mr. Owad concluded, "you had to get a warrant to monitor a person or a group of people. Today, it is increasingly easy to monitor ideas. And then track them back to people."

What Mr. Owad did by hand can increasingly be performed automatically, with data-mining software that draws from many sites and databases. One of the essential characteristics of the Net is the interconnection of diverse stores of information. The "openness" of databases is what gives the system much of its power and usefulness. But it also makes it easy to discover hidden relationships among far-flung bits of data. 9

In 2006, a team of scholars from the University of Minnesota described how easy it is for data-mining software to create detailed personal profiles of individuals — even when they post information anonymously. The software is based on a simple principle: People tend to leave lots of little pieces of information about themselves and their opinions in many different places on the Web. By identifying correspondences among the data, sophisticated algorithms can identify individuals with extraordinary precision. And it's not a big leap from there to discovering the people's names. The researchers noted that most Americans can be identified by name and address using only their ZIP code, birthday and gender — three pieces of information that people often divulge when they register at a website. 10

The more deeply the Net is woven into our work lives and leisure activities, the more exposed we become. Over the last few years, as social-networking services have grown in popularity, people have come to entrust ever more intimate details about their lives to sites like *Facebook* and *Twitter*. The incorporation of GPS transmitters into cellphones and the rise of location-tracking services like *Foursquare* provide powerful tools for assembling moment-by-moment records of people's movements. As reading shifts from printed pages onto networked devices like the Kindle and the Nook, it becomes possible for companies to more closely monitor people's reading habits — even when they're not surfing the Web. 11

"You have zero privacy," Scott McNealy remarked back in 1999, when he was chief executive of Sun Microsystems. "Get over it." Other Silicon Valley CEOs have expressed similar sentiments in just the last few months. While Internet companies may be complacent about the erosion of personal privacy — they, after all, profit from the trend — the rest of us should be wary. There are real dangers. 12

First and most obvious is the possibility that our personal data will fall into the wrong hands. Powerful data-mining tools are available not only to legitimate corporations and researchers, but also to crooks, con men and creeps. As more data about us is collected and shared online, the threats from unsanc- 13

tioned interceptions of
information about our
use locational data to t

The first line of de
sonal responsibility for
amount of caution wil
without our knowledg
online, and how they'
against abuses.

A second danger
to influence our beha
us. Personalization's e
keters refine data-mi
people's behavior as
online ads and othe
Schmidt acknowledg
an algorithm can acc

As marketing p
our past patterns of b
behavior. Already, a
about people by mo
that knowledge to c
A man who visits a
promotional messag
research about anxi
between personaliza
tain: We can never
companies know ab

Safeguarding p
ware makers and sit
tion private. Privac
when companies tr
they should provid

The greatest d
is that it may lead
as outdated and ur
to efficient shopp
puter security exp
we hide behind w
"intrinsic to the
watched, we begi

›ut treating depression or
ded, "you had to get a war-
ıy, it is increasingly easy to
e."

›e performed automatically, 9
ıites and databases. One of
onnection of diverse stores
ıt gives the system much of
ɔ discover hidden relation-

ity of Minnesota described 10
etailed personal profiles of
ınonymously. The software
ave lots of little pieces of
n many different places on
he data, sophisticated algo-
precision. And it's not a big
The researchers noted that
ddress using only their ZIP
ırmation that people often

ıur work lives and leisure 11
ıe last few years, as social-
ople have come to entrust
tes like *Facebook* and *Twit-*
cellphones and the rise of
e powerful tools for assem-
ıvements. As reading shifts
the Kindle and the Nook,
ly monitor people's reading

ıarked back in 1999, when 12
Get over it." Other Silicon
n just the last few months.
ıout the erosion of personal
the rest of us should be wary.

ır personal data will fall into 13
available not only to legiti-
ɔks, con men and creeps. As
ıe, the threats from unsanc-

tioned interceptions of the data grow. Criminal syndicates can use purloined information about our identities to commit financial fraud, and stalkers can use locational data to track our whereabouts.

The first line of defense is, of course, common sense. We need to take personal responsibility for the information we share whenever we log on. But no amount of caution will protect us from the dispersal of information collected without our knowledge. If we're not aware of what data about us are available online, and how they're being used and exchanged, it can be difficult to guard against abuses. 14

A second danger is the possibility that personal information may be used to influence our behavior and even our thoughts in ways that are invisible to us. Personalization's evil twin is manipulation. As mathematicians and marketers refine data-mining algorithms, they gain more precise ways to predict people's behavior as well as how they'll react when they're presented with online ads and other digital stimuli. Just this past week, *Google* CEO Eric Schmidt acknowledged that by tracking a person's messages and movements, an algorithm can accurately predict where that person will go next. 15

As marketing pitches and product offerings become more tightly tied to our past patterns of behavior, they become more powerful as triggers of future behavior. Already, advertisers are able to infer extremely personal details about people by monitoring their Web-browsing habits. They can then use that knowledge to create ad campaigns customized to particular individuals. A man who visits a site about obesity, for instance, may soon see a lot of promotional messages related to weight-loss treatments. A woman who does research about anxiety may be bombarded with pharmaceutical ads. The line between personalization and manipulation is a fuzzy one, but one thing is certain: We can never know if the line has been crossed if we're unaware of what companies know about us. 16

Safeguarding privacy online isn't particularly hard. It requires that software makers and site operators assume that people want to keep their information private. Privacy settings should be on by default and easy to modify. And when companies track our behavior or use personal details to tailor messages, they should provide an easy way for us to see what they're doing. 17

The greatest danger posed by the continuing erosion of personal privacy is that it may lead us as a society to devalue the concept of privacy, to see it as outdated and unimportant. We may begin to see privacy merely as a barrier to efficient shopping and socializing. That would be a tragedy. As the computer security expert Bruce Schneier has observed, privacy is not just a screen we hide behind when we do something naughty or embarrassing; privacy is "intrinsic to the concept of liberty." When we feel that we're always being watched, we begin to lose our sense of self-reliance and free will and, along 18 with it, our individuality. "We become children," writes Mr. Schneier, "fettered under watchful eyes."

Privacy is not only essential to life and liberty; it's essential to the pursuit of happiness, in the broadest and deepest sense. We human beings are not just social creatures; we're also private creatures. What we don't share is as important as what we do share. The way that we choose to define the boundary between our public self and our private self will vary greatly from person to person, which is exactly why it's so important to be ever vigilant in defending everyone's right to set that boundary as he or she sees fit. 19

For a reading quiz, visit bedfordstmartins.com/thebedfordreader.

Journal Writing

"The more deeply the Net is woven into our work lives and leisure activities, the more exposed we become," Carr writes in paragraph 11. What does he mean? And do you agree? In your journal, draft a narrative account of an experience you have had of feeling exposed while using an online medium such as *Google*, *Facebook*, or *Foursquare*. If you've never felt exposed, explain why not. (To take your journal writing further, see "From Journal to Essay" on the facing page.)

Questions on Meaning

1. What problem does Carr identify? What solution, if any, does he propose?
2. How, according to Carr, do "corporations, governments or other outsiders" (par. 2) obtain personal information about individual Internet users? Identify at least two ways.
3. "There are real dangers" to losing privacy online, Carr writes in paragraph 12. What are those dangers, as he sees them?
4. What seems to be Carr's PURPOSE in writing this essay? Is he writing mainly to express a concern, offer a solution to a problem, influence government regulations, change individuals' attitudes, or do something else? What details from the essay support your answer?

Questions on Writing Strategy

1. What does the author accomplish by opening with a discussion of the "tradeoff" (par. 3) between privacy and personalization?
2. Is this essay an appeal to emotion or a reasoned argument, or both? Give evidence for your answer.
3. Why is Carr so concerned about "manipulation" (pars. 15–16)? What exactly does he think could happen if advertisers customize their messages to individ-

ual Internet users' int
What does he seem tc

4. **OTHER METHODS** W
ing of *privacy*? By wh
subject of liberty?

1. How would you desc
TONE of his argumen
2. Why do you suppose
(8), Scott McNealy
these people? What
explain his points?
3. Be sure you are fami
sary: surreptitious (
syndicates, purloine

1. **FROM JOURNAL TO**
journal to write an
the Internet and l
Do you believe th
details about thei
Why, or why not?
2. Both of the nove
George Orwell's N
societies in whicl
iors. Choose one
it), keeping Carr'
represent particul
Carr's purpose ar
about the motive
3. **CRITICAL WRITIN**
of Carr's ideas. S
vacy as desirabl
(12) as he claim
Do we really ne
dence from your
4. **CONNECTIONS**
cations of data
(p. 551) that tr
the author of t
sees little reaso
agree? How do
more convince
most convincir