rumor that Obama attended a madrasa was also called a falsehood, and links were provided to a CNN story depicting his school in Indonesia as a regular elementary school. In response to rumors that Obama was not born in the United States, the site provided a PDF copy of his birth certificate.

While effective at providing Obama supporters and the news media appropriate responses to rumors, FightTheSmears.com was also the subject of significant criticism. According to some psychologists, listing rumors and then rebutting them can often lead readers to remember the rumors as true. Thus, naming false accusations can sometimes give such distortions credibility. Other critics complained that the Web site was often short on evidence, unlike the fact-checking portion of Obama's campaign Web site that preceded FightTheSmears.com. Additionally, the site's effectiveness was further questioned because there was little proof that users would actually forward links to those who believed the rumors. Finally, many conservatives complained that Republicans were too quickly blamed for spreading rumors that were actually started by Obama's opponents in the Democratic primary.

FightTheSmears.com ceased to exist after the 2008 campaign, but it evolved into other Web sites used by the Obama administration. In August 2009, the White House launched WhiteHouse.gov/realitycheck to counter rumors about health insurance reform. The site listed and refuted several rumors—ranging from claims that the Affordable Care Act would lead to rationing of health care services to lies about "death panels"—and asked users to forward suspicious e-mails to flag@whitehouse.gov. In September 2011, the president's campaign launched Attack Watch, along with a Twitter hashtag, to debunk misinformation about the administration. Obama supporters were encouraged to submit reports on smears against the president, mostly by fact-checking Republican presidential candidates. By February 2012, the Obama campaign launched a site for Truth Teams to fight misinformation about the president. Linked to Obama's campaign Web site, Truth Teams listed information by issue and allowed groups of fact-checkers to organize in several swing states.

Ryan Neville-Shepard
Indiana University–Purdue University Columbus

See Also: Campaign Strategy; Campaigns, Presidential (2008); Crowdsourcing; Health Care; Rumors; Truth Team.

Further Readings

DiFonzo, Nicholas. *The Watercooler Effect: A Psychologist Explores the Extraordinary Power of Rumors*. New York: Palgrave Macmillan, 2008.

Garrett, R. Kelly. "Troubling Consequences of Online Political Rumoring." *Human Communication Research*, v.37/2 (2011).

Waggenspack, Beth. "Deceptive Narratives in the 2008 Presidential Campaign." In *Studies of Identity in the 2008 Presidential Campaign,* Robert E. Denton, ed. Lanham, MD: Rowman & Littlefield, 2010.

Findability

Though it has existed for years, findability in its common usage today is a concept popularized by Peter Morville in 2005 to refer to how easily a Web user can find online content using a search engine or by navigating within a particular Web site. To be findable means that it is possible and easy to locate online information known to exist in a general place. In its simplest sense, findability concerns how easy it is for people to find what they are looking for online. Far from a simple concept, though, findability calls upon Web designers and information architects to conceptualize and organize Web content in a way that maximizes its ability to be located, reached, and identified by those looking for it either from within or outside the Web site where it is kept. These organizational choices may have political implications because depending upon one's perspective, it is not always desirable to make certain information easy to find.

On today's Web, search engines play a powerful role in directing Web users toward information thought to be most relevant to a user's search. But search engines offer only limited attentiveness to the nuance of what one may be seeking. Peter Morville, for instance, writes that he was partly inspired to think about findability after searching online for information about his daughter's peanut allergy, only to find that search engines

typically directed him toward overtly commercial Web sites or other marketing material selling nut-free products, which was not the information he wanted. Findability is not just a matter of making it easy to find one's way toward certain information; it is also a matter of assuring the relevance of the information toward which one is directed. While search engine optimization techniques offer Web designers a way to increase the likelihood that their Web sites will appear more prominently in a search engine's results, findability goes further still.

For Morville, findability as a tenet of Web design or information architecture is concerned with three primary questions: "(1) Can your users find your Web site? (2) Can your users find their way around your Web site? (3) Can your users find your products and content despite your Web site?" These three questions might respectively be characterized as problems of locating, reaching, and identifying. In other words, ensuring maximal findability means that a Web user can easily locate the Web site where desired information or content exists, that the user can then navigate easily through the Web site to reach the specific place where this information is kept, and that a Web user can easily and accurately identify the pertinent information as such once he or she has located and reached it.

This last entreaty is especially difficult in a Web with organizational signposts structured with semantic cues that usually amount to key words intended to guide search engines toward particular content. Key words, however, do not always capture the complexity of the content that one may wish to find. Moreover, a clumsy presentation of content on a Web site may unintentionally conceal the relevant information contained therein. That is, it sometimes happens that Web users have arrived at the information they are looking for without realizing it. The desired content may be poorly worded, it may be visually messy, or it may be hidden among long paragraphs full of other information not relevant to the user's concerns. Any variety of reasons—aesthetic, grammatical, or contextual—might make desired content unidentifiable, even in plain sight. Maximizing findability in part means ensuring that information is identifiable for what it is, once a user has arrived at its door.

Findability is not just practical; it can also be political. The concept's political aspect becomes evident when considering that content providers do not always have a motivation to make their content easy to find. Sometimes, a content provider has a vested interest to deliberately hide information or otherwise make it not readily findable. For instance, disclaimers required by law, for example, about the side effects of medications or the dangers of cigarettes might deter consumers from buying those products, even though the law demands such disclaimers. Similarly, Web designers may find it necessary for a Web site to include some content that is unflattering, dry, uninteresting, or otherwise unappealing. In such instances, Web designers make decisions to privilege the visibility (and the findability) of certain classes of information over others in order to be more rhetorically effective. Though findability concerns the ease of finding content or information, its corollary concerns the opposite drive to make information more difficult to find. Nevertheless, findability is not a finite resource. The networked structure of the Web means that making some content findable does not necessarily make other content less findable. Strategic decisions, however, can operate to emphasize the findability of certain content more than others, and it is these decisions that bring findability into the realm of the political.

Far from limited to virtual environments, findability in its broader sense also refers to the intervention of technology as an apparatus to help any wayfinding experience. For instance, handheld or dashboard global position system (GPS) navigational systems, digital mapping of the real world on smartphones, or through applications like Google Earth all contribute to facilitating the ease of making one's way through the world. The concept of findability aspires to make easier what can sometimes be an exasperating process of sorting through an information-saturated world to find exactly what one wants at any given time.

Chris Ingraham
University of Colorado–Boulder
David Spiegel
Institute for Advanced Study

See Also: Information Aggregation; Search and Scrape Capability; Search Engine Optimization.

Further Readings

Morville, Peter. *Ambient Findability*. Sebastopol, CA: O'Reilly Media, 2005.

Morville, Peter. "Ambient Findability: Libraries, Serials, and the Internet of Things." *Serials Librarian*, v.58 (2010).

Thurow, Shari. "Findability, SEO, and the Searcher Experience." *Search Engine Land* (January 21, 2011). http://searchengineland.com/findability-seo-and-the-searcher-experience-61038 (Accessed January 2013).

FinFisher

The increasing pace of globalization and crime requires more effective methods of intervention. Advances in technology offer opportunities for law enforcement agencies to fight crime within national borders. For example, lawful interception is a crucial method used by law enforcement agencies to fight crime. Lawful intervention is the legally sanctioned access of law enforcement agencies of private communications. It provides crucial information regarding what criminal suspects are doing or are planning to do, and is one of the most important tools for law enforcement to fight crime. In some cases, after obtaining a judicial warrant to enter the offices of suspects, law enforcement agencies may have to insert an electronic transmitter called a "bug" into an object belonging to suspects, especially when they are otherwise unable to obtain valuable data about their operations from other sources. In addition, officers often use safe houses or observation cars to receive what is transmitted by these bugs. However, these traditional bugs began to be less functional because of the increased use of computers, smartphones, and tablets. Thus, bugs began to be directly inserted into the devices of suspects or criminals. Intelligence and police officers are currently able to obtain information from electronic devices using software or hardware-based information technology (IT) intrusion bugs to track suspects and criminals.

FinFisher is a UK-based company, a branch of the Gamma Group, which provides IT intrusion solutions for law enforcement agencies. In 2012 and 2013, slivers of information regarding FinFisher products and their unique covert surveillance abilities found their way into several newspaper stories on cyber security, bringing FinFisher technology into limited public view. For example, an analysis conducted by the University of Toronto Munk School of Global Affairs' Citizen Lab regarding five suspicious e-mail attachments obtained by Bloomberg News, which were sent to a Bahraini activist in 2012, exposed the name of FinFisher and its IT intrusion products.

The products that FinFisher provides can be summarized into two groups: those that provide tactical solutions, and those that provide remote intrusion solutions. The term *tactical* refers to the use of equipment by law enforcement officers in the area of operations. In a similar vein, tactical IT intrusion solutions produced by FinFisher are used by law enforcement officers when they are in the vicinity of their targets, or when they have the opportunity for physical access to the IT devices of the targets. *Remote* IT intrusion tools consist of executable codes acting as a Trojan that can covertly access private and personal data of targets and can send them to a remote location by taking remote control of their computers or smartphones. These executable codes are downloaded over the Internet without one's knowledge upon opening an e-mail attachment or text message, or by clicking a link on a Web site. Because they run in the background, they are not noticed by users, unless they are detected by an antivirus program; however, these types of professional codes can bypass many trusted antivirus programs.

These remote IT intrusion tools can secretly record all the text written by the users of a computer or a mobile device as they are striking the keys of the keyboard, and can later send the recorded keystroke history data to a remote location. Furthermore, these tools can access private data sections on the computers and mobile devices of the targets and transmit their private information, documents, and files to a remote location. In addition to taking remote control of the computers, these devices can also provide a means for turning on Web cams and microphones of the computers from a remote location to monitor what the user is doing. Moreover, the smartphone version of the IT intrusion tool can record voice calls and texts, and can track the geographical