

An Analysis of Aggressive Online Behavior Targeted Against Corporations, their Products, Services, and Brands

Urs Gasser
John G. Palfrey, Jr.

May 2007

Table of Contents

Executive Summary	2
1 Introduction	4
2 Three Types of Online Behavior Targeted at Corporations and Other Institutions	5
2.1 Collaborative Behavior.....	6
Minolta, Sony — D7Userforum.de	
Microsoft — IE7 Feedback	
2.2 Socially Constructive Behavior.....	6
Victoria's Secret — Activist Criticism	
Absolut/Adbusters — Spoof Ads	
Unix Haters — Flaming Mailing List	
Coca Cola — Killercoke.org Campaign	
Northwest Airlines — Employee Sickout Campaign	
Apple Inc. — iDont.com	
Microsoft/van Wensveen — Gripe Site	
Lucasnursery — Gripe Site	
McDonald's — McInformation Network	
Starbucks — Gripe Site	
Taubman Co. — taubmansucks.com	
2.3 Aggressive, Destructive Behavior	9
3 Conclusions and Recommendations	12
Methodology	14
About the Authors	15
About the Sponsors	16
Acknowledgments	16
Appendices	17

Executive Summary

The Internet is especially hospitable to those who wish to advance aggressive forms of criticism against corporations and other institutions and who do so in loose collaboration with others, often whom they do not know.

This behavior falls along a continuum of online behavior of three types: (1) collaborative; (2) socially constructive criticism intended as public policy reform; and (3) aggressive, destructive behavior. Each of these types of aggressive behaviors is intended to achieve distinct objectives; is driven by different motivations; and involves the use of different media in the effort to achieve these ends.

1. Collaborative behavior

Often started by product users, brand advocates, beta product testers, etc., this type of behavior is distinguished by its goal of seeking a truly positive outcome for the company and product.

- Objective: to improve a product or service through relevant, honest, timely feedback.
- Motivation: to have an impact by making oneself heard and to improve product quality.
- Media Applications: any convenient online vehicle provided by the corporation perceived to be likely to have someone reading it; blogs and product-specific message boards.

2. Socially constructive behavior

Usually started by activists, non-profit organizations, or disgruntled consumers, this type of behavior is often rooted in social, political, or economic issues that the organizer(s) deeply care about. Companies that listen, evaluate, and respond appropriately to the criticisms and suggestions can prevent these situations from escalating and may even turn them to a benefit.

- Objective: to prompt change on the part of a corporation(s) for perceived public benefit.
- Motivation: to improve society, regardless of negative impact on individual corporations.
- Media Applications: applications with viral potential, including blogs, podcasts, videos, and other media that can be shared and syndicated easily; and sites with message boards.

3. Aggressive, destructive behavior

This is the most negative, insidious type of behavior, often employing the most extreme and disruptive tactics. Companies must respond carefully to such attacks to avoid further inflaming the situation. While legal action is a last resort, there may be some instances where it may be one possible course of action in dealing with this type of behavior.

- Objective: to harm a corporation's brand, to promote oneself, and/or to prompt change.
- Motivation: to work out frustration, to cause harm, to achieve personal fame, and/or to put oneself in a position to make money at the expense of a corporation.
- Media Applications: applications with viral potential, including blogs, podcasts, videos, and other media that can be shared and syndicated easily; and sites with message boards.

CRAFT RESPONSE STRATEGIES TO MATCH THE TYPE OF BEHAVIOR

How a company responds has a great deal to do with the impact of the aggressive behavior. An incorrect response can inflame the aggressive behavior while a correct response may divert the negative behavior.

In responding to aggressive behavior, corporations should consider the following strategies:

Strategy 1: Prevention

Developing systems for monitoring of the relevant user-generated content; ensuring that the right people within the corporation have access to this information; and providing outlets for the frustrations of employees and customers in spaces where the discussion can be constructively handled.

Strategy 2: Early engagement with critics

Identifying the critic's motive and appropriate media application through which to respond. Engagement might involve corporate blogging, despite the challenges, and active engagement in other user-generated content environments. Engagement with online critics is almost always the most effective response.

Strategy 3: Law only as a last resort

Legal action should be a last (not first) resort, and only where there is clear violation of the law involved — not legitimate speech protected by the First Amendment.

1 Introduction

In 1999, two former employees — together with a third accomplice — began a smear campaign on Internet bulletin boards against a biotech company. Today, the bulletin board includes thousands of postings containing false information and allegations against the company and its officers. In November 2005, *Fortune*, a national business magazine in the United States, ran a cover story: “Attack of the Blogs.” In 2006, a Turkish hacker defaced over 38,000 websites in a single day.

In most discussions of Web 2.0 — the buzz-word to describe the interactive phase of Internet development characterized by extensive end-user participation through blogs, wikis, podcasts, vlogs, and other means of self-expression — the emphasis falls upon what is socially beneficial about the shift underway from consumers to creators. The movement toward online user-generated content, and the corresponding decentralization of the media environment, is in many ways good for the health of democracies and markets. “Market are conversations,” said the authors of the break-through book, the *Cluetrain Manifesto*. All this is true — most of the time.

In this paper, we take up the dark side of online behavior. Our frame of reference is from the perspective of institutions — often corporations, but also conceivably universities, NGOs, agencies, and so forth — that are the subject of unusually aggressive online campaigns intended to cause harm to those institutions.

The core aim of this paper is to determine what motivates aggressive online behavior and what, if anything, makes it different than offline aggressive behavior aimed at corporations and other institutions. What drives former employees of a company to devote much of their spare time to organizing online protests against their former employers? What are the most appropriate — and likely to be effective — institutional responses to phenomena such as aggressive online behavior and Internet extremism? Perhaps at the most fundamental level: is there something going on online that is different from criticism of corporations that has gone on offline for as long as business has existed?

In this White Paper, we seek to explore these and related questions. Our orientation is to consider these problems from the approach of a corporation or institution facing such critics, not from the perspective of the critic or from a high-level public policy viewpoint. We approach this problem first at an analytical level (to understand the phenomenon and to set it into a useful context), and then at a normative level (to consider what might be done about it by an institution, but not at the level of public policy).

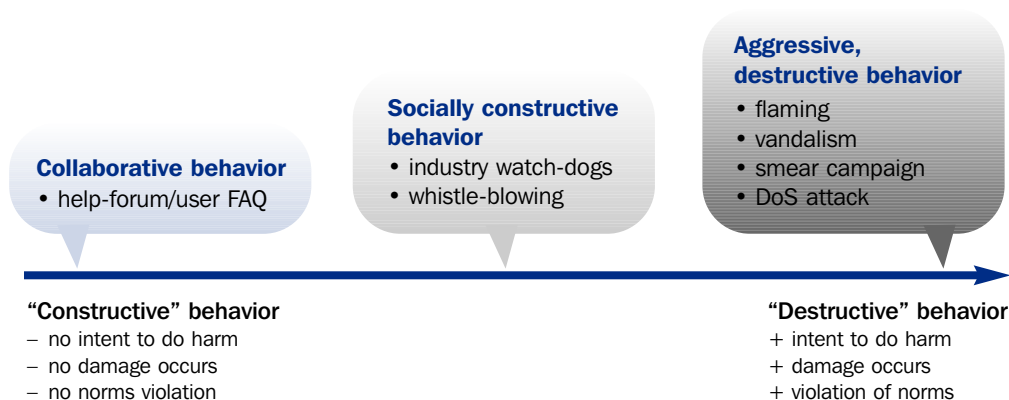
2 Three Types of Online Behavior Targeted at Corporations and Other Institutions

Our inquiry starts with an important principle: aggressive, destructive online behavior must be distinguished from those legitimate forms of expression that are essential to the proper functioning of markets, democracies, and societies at large. By “legitimate” forms of expression, we mean that the activity is protected not just protected by law by the First Amendment in the United States and its analogues around the world, but also that the activity is socially beneficial and does not violate established social norms for acceptable online behavior. Our perspective is that a continuum exists, with constructive behavior on one hand and destructive behavior on the other. Much lies in between.

Online critics often act in this middle ground. The result is that institutions seeking to respond in some fashion to an online critic face a highly complicated situation. In most jurisdictions around the world, legal responses are unlikely to be effective means of addressing the problem, as most online speech (as in the case of other speech) enjoys the protection of the First Amendment or its analogue.. This paper seeks first to map the full spectrum of online behavior targeted against corporations and other institutions, but then to hone in on the behavior on the more aggressive end of the spectrum.

Media psychologists differentiate between various forms of online behavior. These categories include aggressive, discriminating, pro-social, and cooperative behavior. For the purposes of the study, we adopt three main clusters of online behavior that are grouped along a spectrum from what is generally considered to be “constructive” behavior on the one end to what most agree would qualify as “destructive” behavior on the other end of the scale.

The clusters of behavior used in this paper are: (1) collaborative behavior, (2) socially constructive behavior, and (3) aggressive behavior. As the term “cluster” suggests, the characteristics of the three forms of behavior blur towards the edges of the cloud, while the characteristics are clearly distinct at the core of each cluster. The following graph with some examples of different types of behavior might further illustrate the contours of the basic typology suggested here.



2.1 COLLABORATIVE BEHAVIOR

The first cluster is collaborative online behavior. Collaborative behavior can be understood as the interaction between or among two or more individuals who are engaged in actions such as communication, information sharing, coordination, problem solving, or negotiating. Online users can collaborate with companies in many ways. This collaboration can occur in a number of fields and formats. For example, users may be involved in product development, can provide positive or negative feedback on newly released products or services, may write reviews, participate in a FAQ forum, take part in a “viral marketing” campaign, and the like. Although collaborative behavior often involves the publication of “negative” feedback, the sender typically does not seek to cause any damage or harm, but rather seeks to prompt the improvement of a product or service. Usually, collaborative behavior is based upon, and governed by, a shared set of — often-implicit — social norms among the actors. The following examples illustrate this type of collaborative online behavior.

1. Minolta, Sony — D7Userforum.de

In 2002, users of the Minolta Dimage 5, 7x, Ax, Dynax xD and Sony- α cameras organized an independent online forum to exchange news and ideas concerning these products.

2. Microsoft — IE7 Feedback

In the course of developing the latest version of its browser, Microsoft released a beta version of Internet Explorer 7 earlier in 2006. The beta was already the second prototype to be developed and was mainly meant for testing purposes. According to news articles, the release was highly effective from the perspective of the developers’ team. Just hours after the beta went live, bug reports and security warnings started pouring in. For example, while one expert pointed to vulnerability in connection with specifically designed web sites, others found issues with the McAfee anti-virus software and other anti-spyware applications. This voluntary feedback enabled Microsoft to improve its product in a way it could not have done using merely internal tests.

2.2 SOCIALLY CONSTRUCTIVE BEHAVIOR

Socially constructive online behavior is defined as instances where individuals share or make contributions for the benefit of the public at large, with the primary intent of these individuals oriented toward goals larger than the fulfillment of personal ends. Certainly, collaborative behavior is socially constructive, but we distinguish socially constructive behavior as that not explicitly involving cooperation with others.

Examples may take the form of weblogs aimed at informing a specific audience or the public-at-large or photo sharing sites such as Flickr.com. Where such socially constructive behavior concerns or is directed at corporations or other institutions, it may take the form of whistle-blower or

corporate watch-dog sites. In the latter case, the sites may feature positive treatment of corporations alongside negative information, in order to publicize what is deemed to be good corporate behavior. Toward the more antagonistic end of the spectrum fall gripe sites, where an individual or individuals publicize their complaints against or negative experiences with a particular corporation or corporations — but where the primary intention of the speaker is to achieve an end that is purportedly in the public interest. It is important to note that socially constructive behavior can cause considerable pain to a corporation or institution, but if dealt with constructively, can be good for the organization.

This cluster would also encompass a scenario in which a single actor's online posting (not driven by personal financial gain or other factors considered in the third cluster) leads other, unconnected actors to share an opinion. Consider the case of Dell and complaints about its customer service in 2005. The prominent blogger Jeff Jarvis purchased a Dell computer. Jarvis became frustrated by his experience with the product and with the company's responses to his entreaties. In response, he wrote up his experiences and posted his comments to his widely-read blog, BuzzMachine. Jarvis's complaints about Dell's product and customer service snowballed into a much larger outpouring of criticism toward the company. In this case, a large number of customers — unrelated to the initial blogger — felt encouraged to share their own criticism in response to the initial postings of the pied piper, in this case Jarvis. The story also made it into the mainstream press, which further amplified the critiques.

As noted above, the lines between each cluster blur in important and complicated ways. Reasonable people might disagree as to which category should lay claim to certain campaigns. The campaigns cited in this category and in the third category often do not fit neatly into a single category. We roughly categorize a number of examples under the second form of online behavior as follows.

1. Victoria's Secret — Activist Criticism

At least two different social activist groups have targeted the lingerie and clothing label Victoria's Secret. A group of artists put together the website www.whatisvictoriasecret.com, which attempts to portray bulimic women in lingerie, pointing to the deleterious effect on image consciousness which the label's advertising has on young women. Additionally, the organization ForestEthics created www.victoriadirtysecret.net to criticize the use of paper in the label's catalogs.

2. Absolut/Adbusters — Spoof Ads

The website Adbusters featured spoof ads fashioned after the popular Absolut ad campaign in order to draw attention to the dangers of alcohol.

3. Unix Haters — Flaming Mailing List

The "UNIX-Haters" group formed around a mailing list in which programmers and systems administrators shared their complaints and frustrations with the UNIX operating system. As

proprietary software, these complaints may be seen as indirectly aimed at the corporation(s) which owned, developed, and endorsed UNIX. In some instances, contributors even mention specific corporations or corporate products by name (e.g. AT&T, DEC, Sun Microsystems, etc.). UNIX-Haters, however, seems to be less a collection of vitriolic attacks on a particular individual or entity, but rather the legitimate exchange of discovered problems with the operating system.

4. Coca Cola — Killercoke.org Campaign

Social activists used a website to organize worldwide protests against anti-union violence in one of Coca Cola's Colombian bottling plants. The campaign led to the ban of Coke products from major U.S. college campuses. Coke responded with the special website "cokefacts.org." This Killer Coke campaign also became wrapped up in the negative campaigning surrounding the 2006 gubernatorial campaign in Massachusetts, as rival candidates sought to bring down a front-runner by invoking this corporate campaign.

5. Northwest Airlines — Employee Sickout Campaign

In late 1999, flight attendants employed by Northwest Airlines organized a campaign which they dubbed "HAVOC" (Have A Voice in Our Contract). Using a message board on the personal website of a senior flight attendant, Kevin Griffith, the employees organized a large-scale "sickout" which are prohibited by federal labor laws. The goal was to force Northwest to cancel flights during the Christmas holiday season and ultimately due to a deluge of sick calls, 317 flights had to be cancelled between December 30 and January 2

6. Apple Inc. — iDont.com

In May 2006, a competitor of Apple's popular iPod mp3 player set up a website under the heading "idont.com- resist conformity" that is dedicated to fight "the monotony of white earbuds" and reject "the oppressive forces of cultural conformity." On this site, the competitor provides links to satirical or critical movies by third parties about Apple in general and iPods in particular, but also provides its own material such as posters and t-shirt motives, sticker templates, anti-ipod icons, and comics. Furthermore, it advertises its own mp3-player.

7. Microsoft/van Wensveen — Gripe Site

F.W. van Wensveen published a lengthy paper at <http://www.vanwensveen.nl/rants/microsoft/IhateMS.html> complaining of the corporate policies of Microsoft. The site is completely passive, featuring only van Wensveen's paper.

8. Lucasnursery — Gripe Site

A customer published her complaint about the job performed by Lucas Nursery and Landscaping, Inc on the domain "lucasnursery.com." She had registered this domain name and then posted a web page for the sole purpose of reporting her bad experiences to the public and warning other consumers to avoid doing business with the nursery. The nursery brought suit; the former customer's site was deemed protected by the First Amendment.

9. McDonald's — McInformation Network

On February 16, 1996, a group of activists called the McInformation Network launched www.mcspotlight.org. According to its FAQ, the McInformation network is dedicated to “compiling and disseminating factual, accurate, up-to-date (as far as is possible) information, and encouraging debate, about the workings, policies and practices of McDonald’s and other Multinational Corporations.” Among other things, the site offers a guided tour of McDonald’s own website: while the actual mcdonalds.com content is shown in a frame, the corresponding McSpotlight comments can be found right next to it.

10. Starbucks — Gripe Site

The website, ihatestarbucks.com provides a forum for the public-at-large to share their views about Starbucks. A primary page of the site lists the author’s reasons for his or her animus toward the company, which include allegations of unethical corporate practices and bitter coffee. Another page of the site is dedicated to debunking a myth about Starbucks and the Iraq War.

11. Taubman Co. — taubmansucks.com

After being sued by the Taubman Company for creating a neutral site in connection with one of the company’s mall development projects, an individual established a number of gripe sites such as “taubmansucks.com.” Ultimately, the Taubman company’s suit was unsuccessful in establishing Lanham Act liability. Online activist Cory Doctorow amplified the critic’s campaign and resistance to the trademark infringement suit through a posting on the enormously popular blog, Boing Boing.

2.3 AGGRESSIVE, DESTRUCTIVE BEHAVIOR

Generally speaking, one might describe aggressive behavior online as informational situations in which an actor (or “sender,” in information theory terms) violates the rights and/or expectations of others. More precisely, three criteria are common characteristics for aggressive behavior: (1) the sender’s intention to do some kind of harm, (2) the existence of some sort of damage as a result of a sender’s online behavior, and (3) the violation of social and/or legal norms by the sender. Applied to the specific thematic context of this White Paper, these criteria suggests that online behavior usually qualifies as aggressive when an actor intentionally seeks to damage, in one form or another, the reputation or brand of a corporation, where the actions taken are violating social norms (e.g., netiquette) or legal rules (e.g., the Computer Fraud and Abuse Act, a provision of United States federal law that prohibits damaging certain computing equipment), and where the use of media applications negatively affects a corporation (e.g. brand, reputation) or its stakeholders. The following stories might be categorized — to varying degrees — as examples of aggressive behavior.

1. AOL — Reputational Attack on IM

In 1999, a Microsoft employee posed as an independent consultant and sent an e-mail to a security expert, claiming that AIM suffered from security flaws.

2. ADOT / Biomoda — ragingbull.com

Susan Blumenthal, a former employee of a subsidiary of Advanced Optics Electronics (Adot), posted more than 1,200 negative comments on www.ragingbull.com, including allegations of stock fraud by Adot executives between July 2003 and November 2004. ADOT sued Blumenthal for USD 13.5 million because the postings had hurt the stock price of the company. Blumenthal claimed she had merely posted press releases and SEC filings without directly alleging wrongdoing on the part of ADOT and was acting in the public interest. Parties reached settlement after mediation.

3. Genzyme Corporation / Biomatrix — Cybersmearing

When the Genzyme Corporation began contemplating an acquisition of the biotech firm Biomatrix, thousands of accusations and allegations against Biomatrix began to appear on a Yahoo! message board. These allegations appeared even before the deal had been made public. The messages included accusations that officers of Biomatrix had committed various misdeeds and the allegation that the company's leading product had caused the deaths of a number of patients.

4. SSS — System Attack

In January 2006, Richard Benimeli, a computer consultant, accessed the computer system of his former employer "SSS," a call center operator, and manipulated the computer system such that other employees and authorized users were prevented from accessing it. Benimeli previously created a software program used to manage client data and business operations for SSS. Benimeli then demanded 20 % of the value of SSS for his past services and used the attack to extort money from his former employer. In February, 2006, Benimeli was brought up on charges in Cleveland, Ohio.

5. Lufthansa — Denial of Service Attack

On June 20, 2001, Andreas-Thomas Vogel conducted an "online demonstration" against the German air carrier, Lufthansa, by releasing software that coordinated 1.2 million requests to Lufthansa's website from 13,000 computers. As a result, Lufthansa's website was impaired for a period of two hours, preventing ticket purchases through the website's online booking system. Vogel's demonstration was a protest against Lufthansa's cooperation with law enforcement authorities in the forced deportation of asylum seekers which had resulted in the death of one individual.

6. eBay — Denial of Service Attack

In the Summer of 2003, Anthony Scott Clark orchestrated a distributed denial of service attack on eBay with 20,000 computers. He used vulnerabilities in the Windows operating

system and forced eBay and other websites to go offline. Information on his motives for the attack has not become public. Clark was prosecuted under the Computer Fraud and Abuse Act.

7. eBay — Phishing Attack on Customers

Customers of eBay were reportedly subjected to a phishing attack in the Summer of 2006. Customers received an e-mail which asked the eBay customer to confirm, update or verify account data at eBay by clicking on a given link. Upon selecting the link, however, users were then directed to a fraudulent website which mimicked eBay webpages where the phisher could collect personal data.

8. GoDaddy — Website Vandalism

In a single day this year, 38,500 websites, most hosted by the popular and fast-growing web-based service GoDaddy, were vandalized by a Turkish hacker using the handle “iSKORPiTX.” The hacker took advantage of a weakness in the web services security to install a file which would display a Turkish flag with a portrait and the words “HACKED BY iSKORPiTX (TURKISH HACKER)” as well as apparent curses directed at Armenia, Greece, France and “PKK TERROR.”

3 Conclusions and Recommendations

The cases examined in this white paper suggest that companies should prepare for the potential aggressive behavior targeted against them by adopting a set of policies and strategies aimed at preventing, monitoring, planning, and re-evaluating these situations:

- **Invite and engage critics.** The best approach is to create the online outlets for frustrated employees and customers to offer their feedback in a constructive manner. Offer an open door, ideally at your own virtual doorstep — such as feedback tools, discussion forums, rating tools — to facilitate constructive discussions about negative experiences.
- **Create a response plan for each type of behavior.** Corporations should take the time to think through responses ahead of time, creating a scenario plan for each type of aggressive online behavior. The type, motivation, and media used must be evaluated in the response. Aggressive online behavior results from a complex set of interacting emotional and cognitive processes within an individual. Situational variables and a range of motivations
- **Monitor emerging issues.** This planning should be combined with ongoing, active monitoring of user-generated content, to keep tabs on what might emerge. Most aggressive online campaigns involve behavior that fits in more than one category, often shifting over time during a campaign; thus, the monitoring should continue over the entire course of the campaign.
- **Acknowledge the limits of what your response can accomplish.** Aggressive online behavior cannot be “perfectly controlled” by the target of an attack. Neither can aggressive behavior be prevented in all cases. However, corporations often share a certain responsibility not only for the emergence of aggression, but also for the short- and long-term effects of such attacks. As Jonathan Bernstein, the president of Bernstein Crisis Management LLC put it during an interview, “Everybody who carries the brand name into the marketplace is a PR spokesperson, whether you like it or not.” Aggressive behavior is an opportunity for self-observation and self-evaluation by corporate executives.

The framework proposed in this White Paper provides a basis on which to formulate appropriate policies and response strategies to handle different types of aggressive behavior. While the intent of this paper was not to thoroughly examine the entire range of possible responses to create firm guidelines for each scenario, some initial principles emerge:

- **Collaborative behavior:** Where possible, encourage and nurture it. This is one good outlet for frustration that could prevent other, more damaging behavior and improve products and services.

- **Socially constructive behavior:** Even though it can be painful, use it as an opportunity to self-observe and evaluate. To the greatest extent possible, engage critics. They may help you re-evaluate your positions and prompt a change in policy or actions.
- **Aggressive, destructive behavior:** Expect inflammatory language and rhetoric. Don't respond in kind; where possible, re-introduce social cues. In rare cases — for instance, when faced with a denial of service or a phishing attack — legal action may be a part of an overall strategy, especially if the motivation is personal financial gain. If the motivation of the behavior is socio-political, legal action can backfire.

Methodology

We adopted four methodological approaches in this research project. First, we reviewed the existing scholarly literature with respect to the psychology of online behavior, the work of cultural anthropologists, and the (relatively thin) legal scholarship relevant to this topic. Second, we researched a set of exploratory case studies. These cases provide anecdotal evidence for various forms of aggressive online behavior, as well as fertile testing ground for detailed analysis and discussion of these types of behavior and potential counter-measures. Third, we carried out in-depth, questionnaire-based interviews with both actors/activists and representatives of attacked corporations, aimed at contributing to the analysis from a bottom-up perspective. We found, incidentally, that many of those involved in online campaigns involving corporations — whether on the corporate side or on the critic side — were reluctant to be interviewed for this study, even when promised that their identities and specific statements would not be revealed. Some of these interviews took place in person, some on the telephone, and others via the Internet. Finally, we established a series of theoretical frameworks and concepts that we use to describe, evaluate, and better understand aggressive online behavior.

Given the complexity of the core cases we have studied, the White Paper further explores these issues by analyzing and evaluating additional — and in many instances rather specific — stories and cases of online expression targeted at corporations and other institutions, which highlight certain aspects of online campaigns and thus enable us to study the subject in greater detail. Some of these additional cases appear explicitly in this paper; many more do not. This inductive approach to the topic of Internet extremism is meant to enable us to gain a better understanding of the various forces and elements that characterize each of the core components of such campaigns (e.g. types of behavior, motivations, media choice, responses, and so forth) as well as the interactions among these elements.

About the Authors

Urs Gasser is an associate professor of law at the University of St. Gallen, where he serves as the director of the Research Center for Information Law, as well as a faculty fellow of the Berkman Center for Internet & Society at Harvard Law School. Before joining the St. Gallen faculty, Urs spent three years as a research and teaching fellow at the Berkman Center, where he was the lead fellow on the Digital Media Project, a multi-disciplinary research project aimed at exploring the transition from offline/analog to online/digital media. He has published and edited, respectively, six books and has written over 60 articles in books, law reviews, and professional journals. He frequently acts as a commentator on comparative law issues for the US and European media. His blog can be found at <http://blogs.law.harvard.edu/ugasser/>.

John Palfrey is Clinical Professor of Law and Executive Director of the Berkman Center for Internet & Society at Harvard Law School (<http://cyber.law.harvard.edu/>). His research and teaching is focused on the impact of the Internet on society. John teaches courses with a focus on Internet law, intellectual property, e-commerce, and digital democracy. He has published a number of scholarly papers related to the Internet's relationship to Intellectual Property, international governance, and democracy. Along with Professors Jonathan Zittrain and William Fisher, he co-authored an amicus brief to the United States Supreme Court in *MGM v. Grokster*. He is a founder of several technology start-ups, including Top Ten Media, Inc., a Web 2.0 services company, which he serves as Chairman. Prior to joining the Berkman Center, he practiced intellectual property and corporate law at the law firm of Ropes & Gray. He writes a blog found at <http://blogs.law.harvard.edu/palfrey/>.

About the Sponsors

A number of companies provided financial and substantive support for the extensive series of interviews from which the White Paper's conclusions are drawn. These sponsors include Alticor, RSS Labs, and Top Ten Media. This executive version of the White Paper was commissioned by Cymfony.



Cymfony, a TNS Media Intelligence company, tells brands and companies what people are saying about them whether the people are bloggers, traditional journalists or even influential consumers. Cymfony sifts and interprets the millions of voices at the intersection of traditional and social media to gain consumer insights that help companies identify the people, keep on top of the issues and respond to the trends impacting their business — at the speed of the market. We call this approach to harnessing this new dynamic “market influence analytics”.

Cymfony works with marketing, research and PR professionals worldwide, offering range of packaged services that address areas such as consumer-generated media strategy, consumer opinions and trends, customer satisfaction, PR measurement, and reputation management. For more information contact us at 617-673-6000 or info@cymfony.com.

This White Paper is published by the Center for Public Learning. For more information about the Center, please contact Dr. James F. Moore at 66 Church Street, Second Floor, Cambridge, MA 02138 or [jmoore AT newslikemediagroup.com](mailto:jmoore@newslikemediagroup.com). To contact the authors of this White Paper, please write to Urs Gasser at [ugasser AT cyber.law.harvard.edu](mailto:ugasser@cyber.law.harvard.edu) or John Palfrey at [jpalfrey AT law.harvard.edu](mailto:jpalfrey@law.harvard.edu).

Acknowledgments

We acknowledge the research assistance of Malte Ziewitz, M.P.A. (Harvard). Thanks also to Silke Ernst, LL.M., James Thurman, Esq., and Dr. Peter Gasser for help and comments.