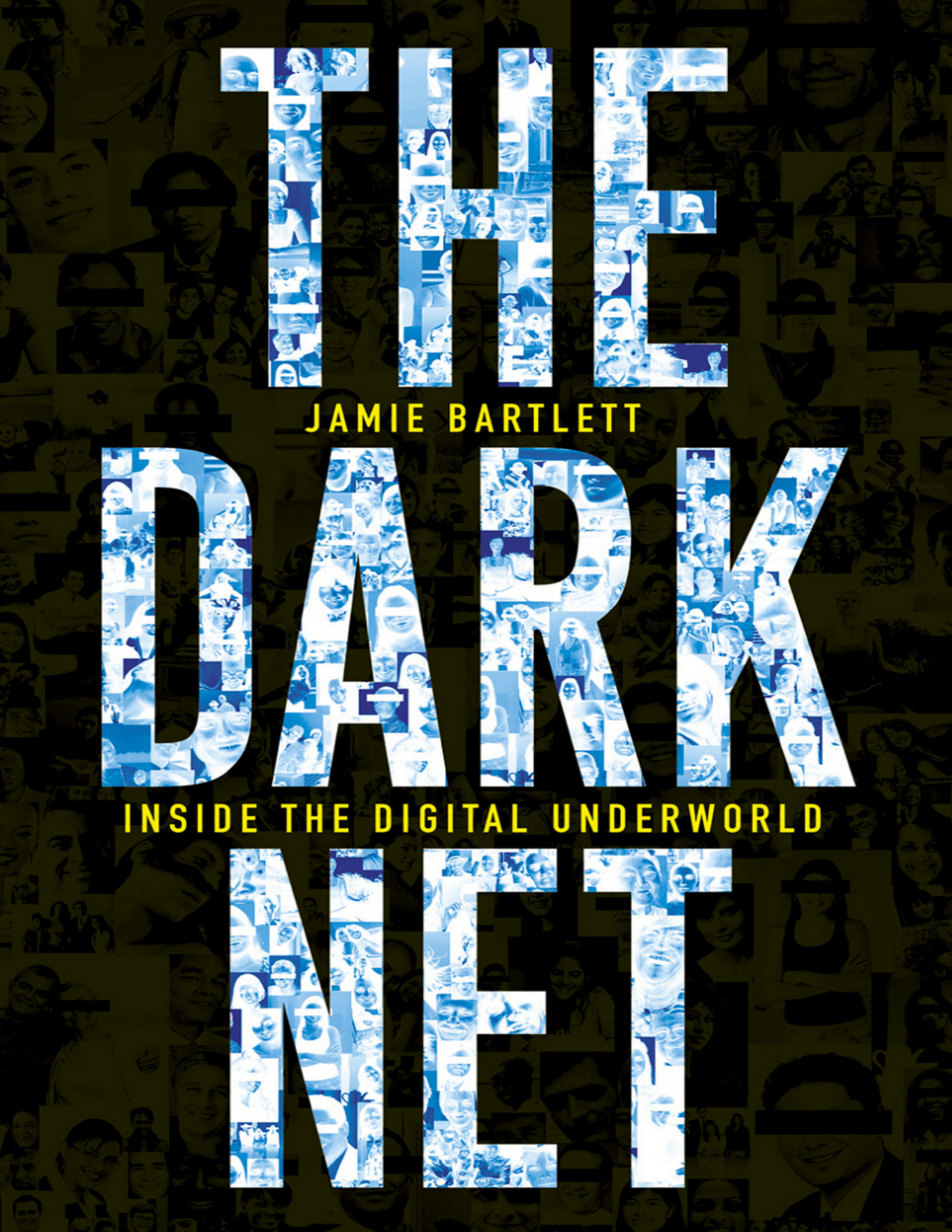
THE
JAMIE BARTLETT
DARK
INSIDE THE DIGITAL UNDERWORLD
NET

Contents

About the Book

Beyond the familiar online world that most of us inhabit – a world of Google, Hotmail, Facebook and Amazon – lies a vast and often hidden network of sites, communities and cultures where freedom is pushed to its limits, and where people can be anyone, or do anything, they want. A world that is as creative and complex as it is dangerous and disturbing. A world that is much closer than you think.

The dark net is an underworld that stretches from popular social media sites to the most secretive corners of the encrypted web. It is a world that frequently appears in newspaper headlines, but one that is little understood, and rarely explored. *The Dark Net* is a revelatory examination of the internet today, and of its most innovative and dangerous subcultures: trolls and pornographers, drug dealers and hackers, political extremists and computer scientists, Bitcoin programmers and self-harmers, libertarians and vigilantes.

Based on extensive first-hand experience, exclusive interviews and shocking documentary evidence, *The Dark Net* offers a startling glimpse of human nature under the conditions of freedom and anonymity, and shines a light on an enigmatic and ever-changing world.

About the Author

Jamie Bartlett is the Director of the Centre for the Analysis of Social Media at the think tank Demos, where he specialises in online social movements and the impact of technology on society. He lives in London.

The Dark Net

Inside the Digital Underworld

Jamie Bartlett

WILLIAM HEINEMANN: LONDON

For Huey, Max, Sonny and Thomas, who were born while I was writing this book. When they are old enough, I hope they will read it and wonder what on earth all the fuss was about, and laugh at their uncle’s hopeless predictions.

Author’s Note

The Dark Net is an examination of what are, in many cases, extremely sensitive and contentious subjects. My primary aim was to shine a light on a world that is frequently discussed, but rarely explored – often for good reason. Throughout I have endeavoured to set my own views aside and write as objective and as lucid an account of what I experienced as possible. Readers may question the wisdom of writing about this subject at all, and express concern at the information *The Dark Net* reveals. Although my intention was never to provide a guide to illegal or immoral activity online, this book does contain material that some readers will find shocking and offensive.

As a researcher I felt a duty to respect the privacy of the people I encountered. Where necessary, I have altered names, online pseudonyms and identifying details, and, in one chapter, created a composite character based on several individuals. For the reader’s ease, I have also corrected many (but not all) spelling mistakes in quoted material.

I have tried to balance the rights of individuals with the social benefit that I believe comes from describing them and the worlds they inhabit. It is not a foolproof method; rather a series of judgements. Any errors, omissions and mistakes are mine alone, and I hope those included in this book will accept my apologies in advance for any distress or discomfort caused.

Online life moves quickly. Doubtless by the time you read *The Dark Net*, certain parts of the story will have changed, websites will have closed down, sub-cultures will have

evolved, new laws will have been enacted. But its core theme – what humans do under the conditions of real or perceived anonymity – will certainly have not.

Jamie Bartlett
July 2014

Introduction

Liberty or Death

I HAVE HEARD rumours about this website, but I still cannot quite believe that it exists. I am looking at what I think is a hit list. There are photographs of people I recognise – prominent politicians, mostly – and, next to each, an amount of money. The site's creator, who uses the pseudonym Kuwabatake Sanjuro, thinks that if you could pay to have someone murdered with no chance – I mean absolutely *zero* chance – of being caught, you would. That's one of the reasons why he has created the Assassination Market. There are four simple instructions listed on its front page:

> >Add a name to the list
> >Add money to the pot in the person's name
> >Predict when that person will die
> >Correct predictions get the pot

The Assassination Market can't be found with a Google search. It sits on a hidden, encrypted part of the internet that, until recently, could only be accessed with a browser called The Onion Router, or Tor. Tor began life as a US Naval Research Laboratory project, but today exists as a not-for-profit organisation, partly funded by the US government and various civil liberties groups, allowing millions of people around the world to browse the internet anonymously and securely.[fn1] To put it simply, Tor works by repeatedly encrypting computer activity and routing it via several network nodes, or 'onion routers', in so doing concealing the

origin, destination and content of the activity. Users of Tor are untraceable, as are the websites, forums and blogs that exist as Tor Hidden Services, which use the same traffic encryption system to cloak their location.

The Assassination Market may be hosted on an unfamiliar part of the net, but it's easy enough to find, if you know how to look. All that's required is a simple (and free) software package. Then sign up, follow the instructions, and wait. It is impossible to know the number of people who are doing exactly that, but at the time of writing, if I correctly predict the date of the death of Ben Bernanke, the former chairman of the Federal Reserve, I'd receive approximately $56,000.

It may seem like a fairly pointless bet. It's very difficult to guess when someone is going to die. That's why the Assassination Market has a fifth instruction:

> >Making your prediction come true is entirely optional

The Dark Net

The Assassination Market is a radical example of what people can do online. Beyond the more familiar world of Google, Hotmail and Amazon lies another side to the internet: the dark net.

For some, the dark net is the encrypted world of Tor Hidden Services, where users cannot be traced, and cannot be identified. For others, it is those sites not indexed by conventional search engines: an unknowable realm of password protected pages, unlinked websites and hidden content accessible only to those in the know. It has also become a catch-all term for the myriad shocking, disturbing and controversial corners of the net – the realm of imagined criminals and predators of all shapes and sizes.

The dark net is all of these things, to some extent – but for me, it is an idea more than a particular place: an underworld set apart yet connected to the internet we inhabit, a world

of complete freedom and anonymity, and where users say and do what they like, uncensored, unregulated, and outside of society's norms. It is a world that is as shocking and disturbing as it is innovative and creative, a world that is also much closer than you think.

The dark net is rarely out of the news – with stories of young people sharing homemade pornography, of cyberbullies and trolls tormenting strangers, of political extremists peddling propaganda, of illegal goods, drugs and confidential documents only a click or two away appearing in headlines almost daily – but it is still a world that is, for the most part, unexplored and little understood. In reality, few people have ventured into the darker recesses of the net to study these sites in any detail.

I started researching radical social and political movements in 2007, when I spent two and a half years following Islamist extremists around Europe and North America, trying to piece together a fragmented and largely disjointed real-world network of young men who sympathised with al-Qaeda ideology. By the time I'd finished my work in 2010, the world seemed to be different. Every new social or political phenomenon I encountered – from conspiracy theorists to far-right activists to drugs cultures – was increasingly located and active online. I would frequently interview the same person twice – once online and then again in real life – and feel as if I was speaking to two different people. I was finding parallel worlds with different rules, different patterns of behaviour, different protagonists. Every time I thought I'd reached the bottom of one online culture, I discovered other connected, secretive realms still unexplored. Some required a level of technical know-how to access, some were extremely easy to find. Although an increasingly important part of many people's lives and identities, these online spaces are mostly invisible: out of reach and out of view. So I went in search of them.

My journey took me to new places online and offline. I became the moderator of an infamous trolling group and spent weeks in forums dedicated to cutting, starving or killing yourself. I explored the labyrinthine world of Tor Hidden Services in search of drugs, and to study child pornography networks. I witnessed online wars between neo-Nazis and anti-fascists on popular social media sites, and signed up to the latest porn channels to examine current trends in home-made erotica. I visited a Barcelona squat with anarchist Bitcoin programmers, run-down working men's clubs to speak to extreme nationalists, and a messy bedroom to observe three girls make a small fortune performing sexually explicit acts on camera to thousands of viewers. By exploring and comparing these worlds, I also hoped to answer a difficult question: do the features of anonymity and connectivity free the darker sides of our nature? And if so, how?

The Dark Net is not an effort to weigh up the pros and cons of the internet. The same anonymity that allows the Assassination Market to operate also keeps whistleblowers, human-rights campaigners and activists alive. For every destructive sub-culture I examined there are just as many that are positive, helpful and constructive.

This book cannot even be considered a comprehensive account of the multitude of darker sub-cultures that permeate online life. From encrypted Tor Hidden Services to popular social media sites, it's difficult to know how deep the rabbit hole goes. This is instead one person's experience of spending an extended period of time in a few of the internet's least explored backwaters, and an attempt to try to understand and explain what takes place there, and why. In the dark net, I came to learn, things are often not what they first appear.

Connected

The net as we know it started life in the late 1960s, as a small scientific project funded and run by the Advanced Research Projects Agency (ARPA), a development arm of the US military. The Pentagon hoped to create an ‘Arpanet’ of linked computers to help top American academics share data sets and valuable computer space. In 1969 the first networked connection was made between two computers in California. It was a network that slowly grew.

In July 1973 Peter Kirstein, a young professor of computer science at University College London, connected the UK to the Arpanet via the Atlantic seabed phone cables, a job that made Kirstein the first person in the UK online. ‘I had absolutely *no* idea what it would become!’ Kirstein tells me. ‘None of us did. We were scientists and academics focused on trying to build and maintain a system which allowed data to be shared quickly and easily.’ The Arpanet, and its successor, the internet, was built on principles that would allow these academics to work effectively together: a network that was open, decentralised, accessible and censorship-free. These ideas would come to define what the internet stood for: an unlimited world of people, information and ideas.

The invention of Bulletin Board Systems (BBS) in 1978, and Usenet in 1979–80, introduced a new generation to life online. Unlike the cloistered Arpanet, Usenet and BBS, the forerunners of the chat room and forum, were available to anyone with a modem and a home computer. Although small, slow and primitive by today’s standards, they were attracting thousands of people intrigued by a new virtual world. By the mid-nineties and the emergence of Tim Berners-Lee’s World Wide Web, the internet was fully transformed: from a niche underground haunt frequented by computer hobbyists and academics, to a popular hangout accessed by millions of excited neophytes.[fn2]

According to John Naughton, Professor of the Public Understanding of Technology at the Open University,

cyberspace at this time was more than just a network of computers. Users saw it as ‘a new kind of place’, with its own culture, its own identity, and its own rules. The arrival of millions of ‘ordinary’ people online stimulated fears and hopes about what this new form of communication might do to us. Many techno-optimists, such as the cheerleaders for the networked revolution *Wired* and *Mondo 2000* magazines, believed cyberspace would herald a new dawn of learning and understanding, even the end of the national state. The best statement of this view was the American essayist and prominent cyberlibertarian John Perry Barlow’s 1996 ‘Declaration of the Independence of Cyberspace’, which announced to the real world that ‘your legal concepts of property, expression, identity, movement, and context do not apply to us . . . our identities have no bodies, so, unlike you, we cannot obtain order by physical coercion.’ Barlow believed that the lack of censorship and the anonymity that the net seemed to offer would foster a freer, more open society, because people could cast off the tyranny of their fixed real-world identities and create themselves anew. (The *New Yorker* put it more succinctly: ‘On the Internet, no-one knows you’re a dog.’) Leading psychologists of the day, such as Sherry Turkle in her influential 1995 study of internet identity, *Life on the Screen*, offered a cautious welcome to the way that online life could allow people to work through the different elements of their identity.

But others worried what might happen if no one knows you’re a dog. Parents panicked about children infected with ‘modem fever’. Soon after Turkle’s study, another psychologist, John Suler, was studying the behaviour of participants in early chat rooms. He found that participants tended to be more aggressive and angry online than offline. He suggested this was because, when protected by a screen, people feel that real-world social restrictions, responsibilities and norms don’t apply. Whether actual or perceived, anonymity, thought Suler, would allow you to

explore your identity, but it might also allow you to act without fear of being held accountable (in 2001 he would call this ‘The Online Disinhibition Effect’). It’s true that from the outset, many BBS and Usenet subscribers were treating cyberspace as a realm for all sorts of bizarre, creative, offensive and illegal behaviour. In Usenet’s ‘Alternative’ hierarchy, anyone could set up a discussion group about anything they wanted. The first group was alt.gourmand, a forum for recipes. This was swiftly followed by alt.sex, alt.drugs and alt.rock-n-roll. ‘*Alt.**’, as it came to be known, immediately became the most popular part of Usenet by far. Alongside purposeful and serious groups for literature, computing or science, Usenet and BBS contained many more dedicated to cyber-bullying, hacking and pornography.

Give Me Liberty or Give Me Death

It was in this heady atmosphere that the radical libertarian Jim Bell first took the promise of online anonymity to a terrifying conclusion. In late 1992, a group of radical libertarians from California called the ‘cypherpunks’ set up an email list to propose and discuss how cyberspace could be used to guarantee personal liberty, privacy and anonymity. Bell, a contributor to the list, believed that if citizens could use the internet to send secret encrypted messages and trade using untraceable currencies, it would be possible to create a functioning market for almost anything. In 1995 he set out his ideas in an essay called ‘Assassination Politics’, which he posted to the email list. It made even the staunchly libertarian cypherpunks wince.

Bell proposed that an organisation be set up that would ask citizens to make anonymous digital cash donations to the prize pool of a public figure. The organisation would award the prize to whoever correctly predicted that person’s death. This, argued Bell, wasn’t illegal, it was just a type of gambling. But here’s the ruse: if enough people were

sufficiently angry with a particular individual – each anonymously contributing just a few dollars – the prize pool would become so large that someone would be incentivised to make a prediction and then fulfil it themselves in order to take the pot. This is where encrypted messages and untraceable payment systems come in. A crowd-sourced – and untraceable – murder would unfold as follows. First, the would-be assassin sends his prediction in an encrypted message that can be opened only by a digital code known to the person who sent it. He then makes the kill and sends the organisation that code, which would unlock his (correct) prediction. Once verified by the organisation, presumably by watching the news, the prize money – in the form of a digital currency donated to the pot – would be publicly posted online as an encrypted file. Again, that file can be unlocked only by a 'key' generated by whoever made the prediction. Without anyone knowing the identity of anyone else, the organisation would be able to verify the prediction and award the prize to the person who made it.

The best bit, thought Bell, was that internet-enabled anonymity safeguarded all parties, except perhaps the killer (and his or her victim). Even if the police discovered who'd been contributing to the cash prizes of people on the list, the donors could truthfully respond that they had never *directly* asked for anyone to be killed. The organisation that ran the market couldn't help either, because they wouldn't know who had donated, who had made predictions or who had unlocked the cash file. But Bell's idea was about more than getting away with murder. He believed that this system would exert a populist pressure on elected representatives to be good. The worse the offender – the more he or she outraged his or her citizens – the more likely they were to accumulate a large pool, and incentivise potential assassins. (Bell believed Stalin, Hitler and Mussolini would all have been killed had such a market existed at the time.) Ideally, no one would need to be killed. Bell hoped the very

existence of this market would mean no one would dare throw their hat into the ring at all. ‘Perfect anonymity, perfect secrecy, and perfect security,’ he wrote, ‘. . . combined with the ease and security with which these contributions could be collected, would make being an abusive government employee an extremely risky proposition. Chances are good that nobody above the level of county commissioner would even risk staying in office.’

In 1995, when Bell wrote ‘Assassination Politics’, this was all hypothetical. Although Bell believed his market would ultimately lead to the collapse of every government in the world, reality hadn’t caught up with his imagination. Nearly two decades later, with the creation of digital currencies like Bitcoin, anonymous browsers like Tor and trustworthy encryption systems, it had, and Bell’s vision was realised. ‘Killing is in most cases wrong, yes,’ Sanjuro wrote when he launched the Assassination Market in the summer of 2013:

> However, this is an inevitable direction in the technological evolution . . . When someone uses the law against you and/or infringes upon your rights to life, liberty, property, trade or the pursuit of happiness, you may now, in a safe manner from the comfort of your living room, lower their life-expectancy in return.

There are, today, at least half a dozen names on the Assassination Market. Although it is frightening, no one, as far as I can tell, has been assassinated. Its significance lies not in its effectiveness, but in its existence. It is typical of the sort of creativity and innovation that characterises the dark net: a place without limits, a place to push boundaries, a place to express ideas without censorship, a place to sate our curiosities and desires, whatever they may be. All dangerous, magnificent and uniquely human qualities.

---

fn1 In 2010 Tor was awarded the Free Software Foundation’s Award for Projects of Social Benefit, in part for the service it provides for whistleblowers, human-rights campaigners and activists in dissident movements.

fn2 September 1993, the month America On-Line started to offer its subscribers access to Usenet, is etched into internet folklore as ‘the eternal September’, when newcomers logged on to the internet en masse.

Chapter 1

Unmasking the Trolls

‘At the top of the tree of life there isn’t love: there is lulz.’

Anonymous

A Life Ruin

‘HI /B/!’ READ the small placard that Sarah held to her semi-naked body. ‘7 August 2013, 9.35 p.m.’

It was an announcement to the hundreds – thousands, perhaps – of anonymous users logged on to the infamous ‘/b/’ board on the image-sharing website 4chan that she was ready to ‘cam’. Appreciative viewers began posting various sexually explicit requests, which Sarah performed, photographed and uploaded.

On 4chan, there are boards dedicated to a variety of subjects, including manga, DIY, cooking, politics and literature. But the majority of the twenty million people who visit the site each month head for /b/, otherwise known as the ‘random’ board. Sarah’s photographs were only part of one of many bizarre, offensive or sexually graphic image ‘threads’ constantly running on /b/. Here, there is little to no moderation, and almost everyone posts anonymously. There is, however, a set of loose guidelines: the *47 Rules of the Internet*, created by /b/users, or ‘/b/tards’, themselves, including:

Rule 1: Do not talk about /b/

> Rule 2: Do NOT talk about /b/
>
> Rule 8: There are no real rules about posting
>
> Rule 20: Nothing is to be taken seriously
>
> Rule 31: Tits or G[et] T[he] F[uck] O[ut] – the choice is yours
>
> Rule 36: There is always more fucked-up shit than what you just saw
>
> Rule 38: No real limits of any kind apply here – not even the sky
>
> Rule 42: Nothing is sacred

The anonymous and uncensored world of /b/ generates an enormous amount of inventive, funny and offensive content, as users vie for popularity, and notoriety. Did you ever click on a YouTube link and unexpectedly open Rick Astley's 1987 smash hit 'Never Gonna Give You Up'?[fn1] That was /b/. Or receive funny photographs of cats with misspelled captions? Also /b/. The hacktivist group Anonymous? /b/ again.

But anonymity has its downside. Female users are a novelty here, and are routinely ignored or insulted, that is unless they post photographs of themselves, or play 'camgirl', which is always a simple and effective way to capture the attention of the /b/ tards. 4chan has a dedicated board for camming, called '/soc/', where users are expected to treat camgirls nicely. Every day, dozens of camgirls appear there and perform. But occasionally one foolishly strays into /b/.

Approximately twenty minutes after the first photograph was posted, one user requested that Sarah take a naked photograph of herself with her first name written somewhere on her body. Soon afterwards, another user asked for a naked photograph of her posing with any medication she was taking. She duly performed both tasks. This was a mistake.

> **Anonymous said:** shit, I hope no one doxxes her. She actually delivered. She seems like a kind girl.

Anonymous replied: dude get a grip she gave her first name, her physician's full name, and even the dormitory area she lives in she wants to be found.

Anonymous replied: She is new. Any girl who makes signs or writes names on her body is clearly new to camwhoring, so they really don't know what they're getting themselves into.

Sarah had inadvertently provided enough personal information to allow users to 'dox' her – to trace her identity. Other /b/tards were alerted and quickly joined the thread – on 4chan, doxing a camwhore is seen as a rare treat – and before long, users had located Sarah on her university's searchable directory, and revealed her full name, address and telephone number. Next, they tracked down her Facebook and Twitter accounts. Sarah was still at her computer, watching helplessly.

Anonymous said: STOP. Seriously. Fucking fat losers

Anonymous replied: good to see you're still in the thread sarah. You're welcome btw.

Anonymous replied: heyyy . . . sarah . . . can I add you on facebook? Just kidding delete that shit before your nudes get sent to your friends

Anonymous said: She literally just made her fucking twitter private while I was browsing her pics. Fucking cunt.

Anonymous replied: It's K if she does delete it. I'm making notes on the people on her friends list and their relation with her. Will start sending the nudes soon.

Anonymous replied: LOL she deleted her Facebook. Doubt she can delete her relatives though.

Anonymous replied: Eh, just save her name. Eventually once all this settles she will reactivate it and she will have her jimmies rustled once more. She will now never know peace from this rustling. And she's going to have one embarassing fucking time with her family.

Anonymous said: You fucking nerdbutts got her Facebook? You guys are fucking unbelievable. A girl actually delivers on this shit site, and you fuckers dox her. Fucking /b/, man.

Anonymous replied: get the fuck out you piece of shit moralfag trash

Anonymous replied: How much time do you spend here? You're really surprised by this?

Anonymous said: Those who deliver nudes deserve no harm

Anonymous replied: hahahahahahaha you must be new here. 'for the lulz'.*

Anonymous said: I don't wanna be a whiteknight, but already being one, I wonder why /b/ does this. She provided tits and shit, yet 'we' do this to her. Internet hate machine at its best.

Anonymous replied: /b/ camwhoring: 2004–2013. R.I.P. Thanks.

Anonymous replied: The amazing thing to me is how you guys never shut up about how 'if u keep doxing them we wont have any camwhores left :(.' notice that you've been saying this for roughly a decade.

Anonymous said: Anyway here is a list of all her Facebook friends. You can message friends, and all their own friends, so that anyone with a slight connection to sarah via friend of friend knows

Anonymous replied: So has somebody started messaging her friends and family or can I begin with it?

Anonymous replied: Assume no one else has, because anyone else who responds might be a whiteknight looking to make you think that someone else was already sending the pics out.

Anonymous replied: gogogo

One user created a fake Facebook account, put together a collage of Sarah's pictures, and began sending them to Sarah's family and friends with a short message: 'Hey, do you know Sarah? The poor little sweetie has done some really bad things. So you know, here are the pictures she's posted on the internet for everyone to see.' Within a few minutes, almost everyone in Sarah's social media network had been sent the photographs.

Anonymous said: [xxxxx] is her Fone number – confirmed.

Anonymous replied: Just called her, she is crying. She sounded like a sad sad sobbing whale.

Anonymous replied: Is anyone else continuously calling?

This was what /b/ calls a ‘life ruin’: cyberbullying intended, as its name suggests, to result in long-term, sustained distress. It’s not the first time that /b/ has doxed camgirls. One elated participant celebrated the victory by creating another thread to share stories and screen grabs of dozens of other ‘classic’ life ruins, posting photographs of a girl whose Facebook account had been hacked, her password changed, and the explicit pictures she’d posted on /b/ shared on her timeline.

> **Anonymous said:** I feel kinda bad for her. She was hot and shit, also cute. Too bad she was dumb enough to leak her name and whatnot. Oh, well. Shit happens.
>
> **Anonymous replied:** If was clever she would have g[ot] t[he] f[uck] o[ut] she didnt, therefore she deserves the consequences
>
> **Anonymous replied:** I don’t give a shit what happens either. Bitch was camwhoring while she had a boyfriend.

The operation took under an hour. Soon, the thread had vanished, and Sarah was forgotten.

Doxing camgirls is only one of a growing number of ways that people abuse, intimidate, provoke, anger or ‘troll’ others online. Celebrities, journalists, politicians, sportspeople, academics – indeed, almost anyone in the public eye, or with a large following online – regularly receive insults, inflammatory comments and threats from complete strangers. In 2011, Sean Duffy was imprisoned after making offensive remarks on Facebook, including a post mocking a fifteen-year-old who’d committed suicide. When journalist Caroline Criado-Perez and others succeeded in a campaign to get Jane Austen featured on the new ten-pound note in 2013, she was bombarded with abusive messages from anonymous Twitter users, culminating in bomb and death threats deemed serious enough for the police to advise she move to a safe house. After appearing on BBC’s *Question Time*, the University of Cambridge

classicist Mary Beard received ‘online menaces’ of sexual assault. In June 2014, the author J. K. Rowling was viciously attacked online for donating £1 million to the ‘Better Together’ campaign to oppose Scottish independence.

Some form of trolling takes place on almost every online space. YouTube, Facebook and Twitter all have their own species of troll, each evolved to fit their environment, like Darwin’s finches. MySpace trolls have a register and tone perfectly adapted to upset aspiring teenage musicians. Amateur pornography websites are populated with trolls who know precisely how to offend exhibitionists. The ‘comment’ sections on reputable news sites are routinely bursting with insults.

Over the last five years, there seems to have been a dramatic increase in this type of behaviour. In 2007, 498 people in England and Wales were convicted of using an electronic device to send messages that were ‘grossly offensive, indecent, obscene or of a menacing character’. By 2012, that number had risen to 1,423. Almost one in three eighteen- to twenty-four-year-olds in Britain knows someone who has been a victim of anonymous online abuse. In a poll of almost 2,000 British adults on the subject, 2 per cent said that they had insulted someone, in some form, online – which, when extrapolated, would amount to some one million trolls in the UK alone.

‘Trolling’ has today become shorthand for any nasty or threatening behaviour online. But there is much more to trolling than abuse. Zack is in his early thirties, and speaks with a soft Thames Estuary accent. He has been trolling for over a decade. ‘Trolling is *not* about bullying people,’ he insists, ‘it is all about unlocking. Unlocking situations, creating new scenarios, pushing boundaries, trying ideas out, calculating the best way to provoke a reaction. Threatening to rape someone on Twitter is not trolling: that’s just threatening to rape someone.’

Zack has spent years refining his trolling tactics. His favourite technique, he tells me, is to join a forum, intentionally make basic grammatical or spelling mistakes, wait for someone to insult his writing, and then lock them into an argument about politics. He showed me one recent example that he'd saved on his laptop. Zack had posted what appeared to be an innocuous, poorly written comment on a popular right-wing website, complaining that right-wingers wouldn't be right wing if they read more. An incensed user responded, and then posted a nude picture that Zack had uploaded to an obscure forum using the same pseudonym some time before.

The bait had been taken. Zack hit back immediately:

> You shouldn't deny yourself. If looking at the pics makes you want to touch your penis then just do it . . . if you want I can probably find you some more pictures of my penis – or maybe you'd like some of my ass also? Or if you want we could talk about why regressive ideologies are a bad idea in general and why people who adopt them are likely to have a much harder time in understanding the world than someone who's accepting of progress and social development?

Zack then began posting a series of videos of his penis in various states of arousal interspersed with insults about right-wingers and quotes from Shakespeare and Cervantes. 'Prepare to be surprised!' Zack said mischievously, before he showed me the posts.

For Zack, this was a clear win. His critic was silenced by the deluge, which occupied the comments section of the website for several hours. 'He was so incapable of a coherent response that he resorted to digging into my posting history for things he thought might shame me – but I'm not easily shamed.'

'But what was the point?' I asked him.

There's a short pause. 'I dunno, but it was fun. It doesn't really matter if it was otherwise fruitless.'

For Zack, trolling is part art, part science, part joke, part political act, but also much more. 'Trolling is a culture, it's a

way of thinking’ – and one, he says, that has existed since the birth of the internet. If I wanted to discover where this apparently modern problem came from, I had to go back to the very beginning.

Finger

The internet’s precursor, the Arpanet, was, until the 1980s, the preserve of a tiny academic and governmental elite. These ‘Arpanauts’, however, found that they enjoyed chatting as much as exchanging data sets. Within four years of its creation the Arpanet’s TALK function (originally designed as a small add-on to accompany the transfer of research, like a Post-It note) was responsible for three quarters of all Arpanet traffic. TALK, which later morphed into electronic mail, or ‘e’-mail, was revolutionary. Sitting at your computer terminal in your department building, you could suddenly communicate with several people at once, in real time, without ever looking at or speaking to them. The opportunities afforded by this new technology occasionally made the small group of world-class academics behave in strange ways.

One research group, formed in 1976, was responsible for deciding what would be included in an email header. They called themselves the ‘Header People’, and created an unmoderated chat room to discuss the subject. The room became famous (or infamous) for the raucous and aggressive conversations held there. Arguments could flare up over anything. Ken Harrenstien, the academic who set up the group, would later describe them as a ‘bunch of spirited sluggers, pounding an equine cadaver to smithereens’.

In 1979, another team of academics were at work developing a function called ‘Finger’, which would allow users to know what time other users logged on or off the system. Ivor Durham from Carnegie Mellon University proposed a widget to allow users to opt out of Finger, in

case they preferred to keep their online activity private. The team debated the merits of both sides, but someone leaked the (internal) discussion to the rest of the Arpanet. Durham was attacked relentlessly and mercilessly by other academics from across the US, who believed that this compromised the open, transparent nature of the Arpanet.

Most of these academics knew each other, so online arguments were tempered by the risk of bumping into your foe at the next computer science conference. Nevertheless, misunderstanding and righteous indignation spread across the Arpanet. One participant in the Finger episode thought that tongue-in-cheek comments were usually misread on a computer, and proposed that sarcastic remarks made on the Arpanet be suffixed with a new type of punctuation to avoid readers taking them the wrong way: ;-) But even the first emoticon wasn't enough, because users just started slotting them after a sarcastic put-down, which was somehow even more annoying. ('The f***ing a**hole is winking at me as well?!') Worried that the network was quickly becoming an uncivil place, Arpanauts published a 'netiquette' guide for newcomers. Satire and humour, it advised, was to be avoided, as 'it is particularly hard to transmit, and sometimes comes across as rude and contemptuous'.

Flaming on BBS

In 1978, Ward Christensen and Randy Suess invented the dial-up Bulletin Board System. With a modem, telephone and computer, anyone could either set up or connect to a 'BBS' and post messages. From the early 1980s onwards, BBS was many people's first experience of life online.

Within a year, insulting strangers on boards became a widely acknowledged and accepted part of BBS. Finger and Header Group disputes were more often than not heated debates between academics. But here, people started joining groups and boards with the sole purpose of starting

an argument. This was called ‘flaming’: provoking strangers, disrupting other groups and creating tension for the fun of it. The best ‘flames’ were well written: subtle, clever and biting. Good flamers (who would often post under a pseudonym) built a reputation; people would eagerly await their posts, and archive their best lines. This was more than simple nastiness. For many flamers, it was an opportunity to experiment, to push boundaries, and to have their efforts read and appraised. One prominent flamer even published a guide – ‘Otto’s 1985 Guide to Flaming on BBS’ – advising potential flamers that being as controversial as possible was ‘the only way that people will read your opinions’. ‘It is very hard’, Otto wrote, ‘to ignore a board-wide or NET-wide flame war.’

Dedicated groups started to appear to discuss how to most effectively flame others. In 1987, one BBS user called Joe Talmadge posted another guide, the ‘12 Commandments of Flaming’, to help flamers old and new develop their style:

> Commandment 12: When in doubt, insult. If you forget the other 11 rules, remember this one. At some point during your wonderful career as a Flamer you will undoubtedly end up in a flame war with someone who is better than you . . . At this point, there’s only one thing to do: INSULT THE DIRTBAG!!! ‘Oh yeah? Well, your mother does strange things with vegetables.’

BBS groups were controlled by a systems operator (sysop), who had the power to invite or ban users, and delete flames before they reached the victim. Often labelled censorsops, they were themselves the targets of a nasty strand of flaming called ‘abusing’. Abusers would torment the sysop with insults, spam or anything else they could think of. Sometimes abusers and flamers would ‘crash’ a board with bugs, or post links to Trojan viruses disguised as pirated arcade games for unsuspecting users to download. Another trick was to upload messages referring to pirating, in order to direct snooping authorities towards the unsuspecting sysop.