



5 Steps To Anonymous Online Speech

A Political Activist's Guide

Bill Rounds, Esq.



HowToVANISH.com

Table of Contents

Introduction.....	1
Step 1 - Protect Your IP Address.....	6
Step 2 - Anonymous Email.....	11
Step 3 - Anonymous Domain Name Registration...14	
Step 4 - Anonymous Web Hosting.....	20
Step 5 - Anonymous Donations.....	23
Conclusion.....	26

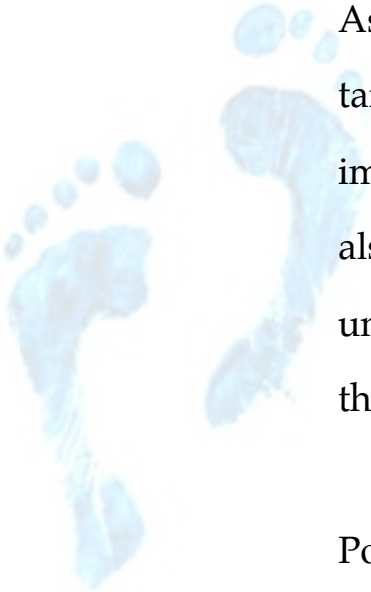
Legal Disclaimer: This information is intended for general information only and is not legal advice. You would have to be crazy to think you are getting legal advice for \$5. We do not make any warranties about completeness reliability and accuracy of this information. No privacy strategy is guaranteed. Any action you take upon this information is strictly at your own risk and we will not be liable for any losses and damages in connection with the use of it. We strive to provide helpful resources from ethical sources and links to useful information, but we have no control over the practices or nature of those resources or links and listing them does not imply a recommendation. Do your own due diligence before using any of their products or services.



“Freedom of the press is guaranteed only to those who own one.”

Abbott Joseph Liebling

Introduction



Political speech is dangerous. From Galileo to Julian Assange, those who criticize powerful people become a target. Political activists have suffered intimidation, imprisonment, torture, and death for centuries. They have also endured a wide range of other less brutal, but equally unjust, forms of retaliation for their speech, like seizure of their property, extortion and censorship.

Political activists can be pressured because they can be identified. If the speaker cannot be identified, no direct pressure can be brought upon them.

Ideas do not always need an identity to spread. There are many cases throughout history where anonymous or pseudonymous speech has had a real effect. One of the most prominent examples is the anonymous publication of *Common Sense*, which was treasonous to publish at the time. It was the best seller, by percentage of population, in the history of the US and convinced large numbers of people to support independence from Britain. The author, Thomas Paine, was not known until after publication.

Sometimes an author *must* remain anonymous to share information. The crimes of Watergate might have never been revealed if Deep Throat could not have remained anonymous.

Laws are insufficient to protect political activists from being unjustly targeted for political speech. All over the world, political activists have been victims of violence because they were not anonymous. Few of them ever make the news in the US, but one who did, [Wael Ghonim](#), was arrested for rallying opposition on Facebook to the Mubarak regime in Egypt. There are hundreds like him with similar stories.

Even in the US, where the law is supposed to protect political speech, there is a long history of violence against political activists. [Civil rights workers](#) in 1960's Mississippi were murdered. More recently, high ranking politicians in the US government called for charges of [treason and the death penalty for Bradley Manning](#), the person suspected of exposing US military misconduct to Wikileaks.

Secrets are safe with no-one. A confidant can be pressured to reveal information about your identity.

In order to criticize any government policy, expose corruption, or uncover embarrassing facts, political activists need to take steps to protect their identity to prevent harassment, imprisonment, and even assassination. The best way for political activists to protect themselves is to publish their information without revealing their identity to anyone.

Fortunately, technology allows political activists to share their ideas and their information anonymously. They can create a website without ever revealing their identity to anyone.

Some very technical people, like members of Anonymous and Lulzsec, will use very advanced techniques to protect their privacy when publishing online. Although no method is bullet proof, for those who are not as technically savvy, there are still very powerful techniques that are extremely simple, very practical, and can provide very solid anonymity when publishing online.

Not all jurisdictions protect free speech in the same way, so some of these techniques may be illegal in some places. Some of these techniques may violate the user agreement of certain companies and service providers. Do not violate the law that applies to you. You are only asking for more trouble if you do. There are usually legal alternatives that will work just as well.

Also, don't violate the user agreement of any service provider. Violating a user agreement is not a criminal act, but the service provider may cancel your service at any time. There will be plenty of alternative service providers that allow you to do what you want without violating their user agreement.

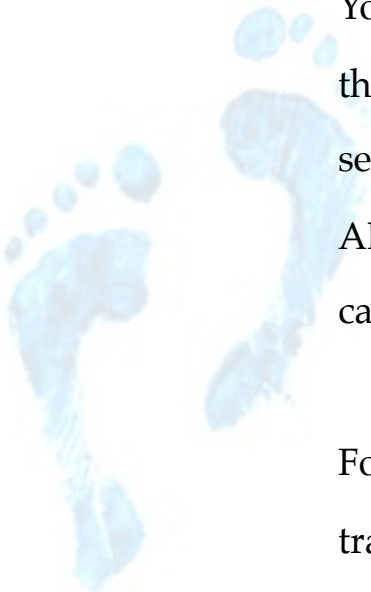
Following is a 5 step system for political activists to publish their message online without fear of being identified.



"I detest what you write, but I would give my life to make it possible for you to continue to write."

Voltaire

Step 1 - Protect Your IP Address



Your IP address can be used to identify you. Websites record the IP addresses that have visited them. Emails that you send will contain information about your IP address. Allowing your IP address to be recorded in various places can leave an electronic trail leading right back to you.

Fortunately, there are three simple ways to prevent being tracked with your IP address, keeping your true identity secret. You should use one or more of these techniques every time you conduct any activity related to your sensitive online political speech like registering your domain name,

signing up for web hosting, sending emails, posting articles, or editing your website.

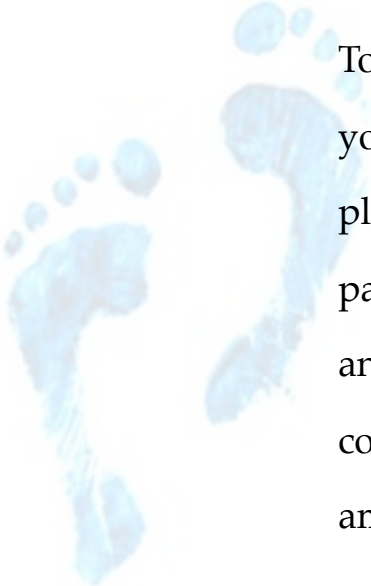
1. Public Wi-Fi Hotspots

Use public Wi-Fi whenever you do anything related to your anonymous website. Coffee shops, libraries, hotels and other businesses offer free internet access to anyone with a laptop. When you use an open Wi-Fi connection, you are using an IP address that is open to anyone. Websites you visit and emails you send will record the publicly available IP address that anyone can use. There is nothing that directly identifies you when you use a public network for online activities.

Don't create any record that identifies you as having used the Wi-Fi hotspot. The users of the public Wi-Fi can still be identified by other means. When IP addresses are captured by the websites you visit, they are also recording the time that you visited the site. Even if the IP address is open to the public, if you have left other records of your presence around the same time, you could still be identified and be

subject to political persecution.

You might be identified if you buy something with your credit card or check around the same time you are using their public Wi-Fi network to conduct website business. Surveillance cameras could record images of your face as you blog away about political ideas. Identification through these indirect methods will be tedious, expensive, and not very common, but it will be possible. These methods of forensic identification have been used to identify individuals using open WiFi in other situations.

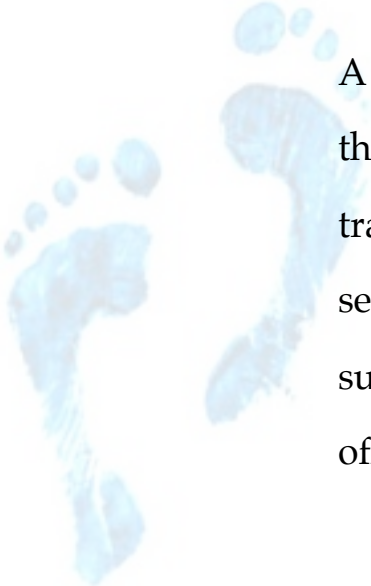


To prevent indirect identification, pay for things in cash if you buy anything from the public Wi-Fi provider. Sit in a place where the surveillance cameras can't see you, like the parking lot or in the restaurant next door. If you do go in and buy things, don't do it around the same time you will be conducting website business. It may also be helpful to rotate among several locations that offer free Wi-Fi.

2. Use Tor

[Tor](#) routes internet traffic through several nodes, making it hard to figure out your IP address, protecting your identity. It makes surfing the internet, visiting websites, sending email and updating your subversive blog, more anonymous. Tor may be much easier to use on a regular basis than using open Wi-Fi hotspots because you can use Tor from the comfort of your own home. You don't need to run down to the local coffee shop and log onto the open WiFi every time you want to post an article. Plus, it's free.

3. Use a VPN



A VPN allows you to access another computer that will surf the web for you. Some VPNs will not anonymize your traffic, but others will. Although there are some VPN services that are free, the most trustworthy ones charge a subscription fee, usually around \$10 - \$20 per month and offer much better service.

A VPN provider could be pressured to reveal your identity. They may have your IP address in their records and they may have payment records which could contain your name.

Step 1 - Protect Your IP Address

The best way to limit this exposure is to take advantage of multiple jurisdictions, something that is very easy to do electronically. Some VPNs route traffic through multiple legal jurisdictions, making it very difficult for one corrupt government to unravel the entire chain. Simply using a VPN based outside of the jurisdiction that you are criticizing can help prevent misuse of the legal process to identify you in customer or payment records.

Use any one, or all three, of these methods EVERY SINGLE TIME you do anything for your website.



VPN RESOURCES

[Cryptohippie](#) – US (Routes traffic through multiple jurisdictions)

[HideMyAss](#) – UK

[Identity Cloaker](#) – Czech Republic (PC Only)

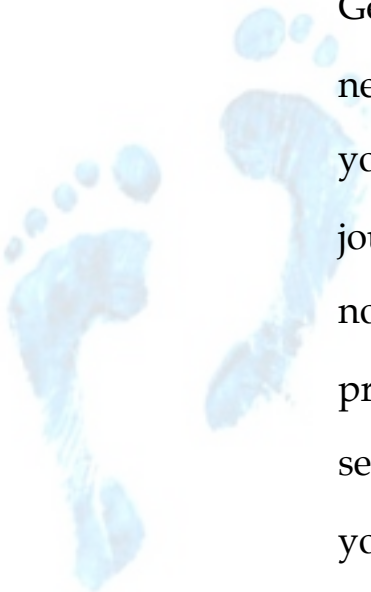
[Witopia](#) – US

[Check out more VPN reviews](#)

"If we don't believe in freedom of expression for people we despise, we don't believe in it at all."

Noam Chomsky

Step 2 - Anonymous Email



Get an anonymous email address. You will almost always need to use an email address to communicate with all of your website service providers, with readers, and with your journalistic sources. You will need an email address that is not connected in any way to your own name. Some email providers will ask for personally identifying information to set up an email address. If you provide it, it is one way that your identity can be revealed.

You may be able to provide a pseudonym to many of the email providers that ask for personally identifying

information. There are very few places where a real name is required by law. You cannot use a pseudonym to commit fraud or some other crime, for example. Pseudonymous information is almost always legal to provide. This applies not only to email, but to almost any situation that requires you to use a name.

Some service providers, like Gmail or Yahoo, do not permit users to use a pseudonym in their terms of service. Although it is not a criminal offense to give them a pseudonym, by violating the terms of service they can cancel your account at any time. There is no reason to use a pseudonym if it violates the user agreement because there are plenty of alternatives to legally protect your privacy.

It may be best to use an email provider that doesn't even ask for personally identifying information to set up an account. Use your anonymous email account for all correspondence regarding website business.

DON'T FORGET to be using a public Wi-Fi hotspot, Tor, or a VPN when you sign up for your anonymous email account and every time you log into your email account.

DO NOT use this anonymous email address for anything personal. Don't tell friends or family that it is you. Don't sign up to get a free t-shirt using your name and this email. Don't forward mail to or from your other personal accounts.

EMAIL RESOURCES

HideMyAss.com

Mail.com

PrivacyHarbor.com

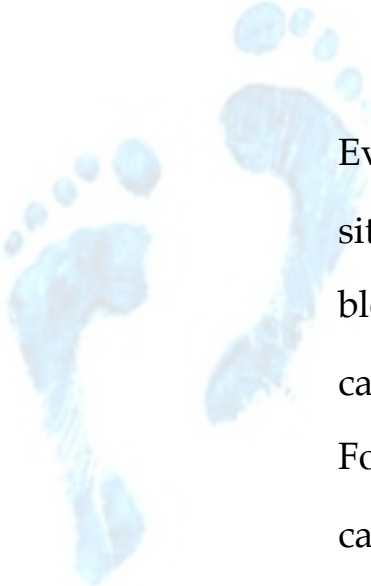
FastMail.fm



"The Internet is an information age tool that empowers individuals and reduces the need for a large, authoritarian government... Unfortunately, it's all a big threat to those in power who rely on the control of information to secure their lofty positions."

Wayne Laugesen

Step 3 - Anonymous Domain Name Registration



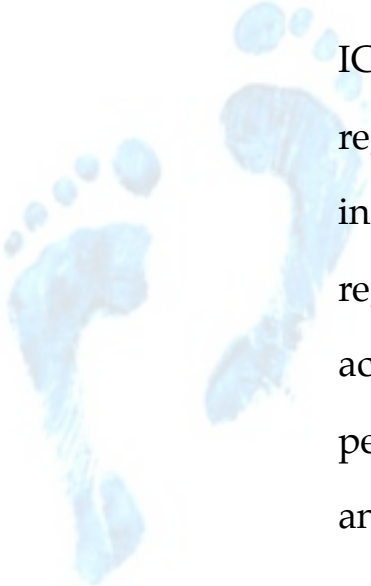
Every website needs a domain name. There are some free sites that let you create your own website for free. You can blog, upload photos and more. Those free website services can be used as Step 3 and Step 4 to protect your anonymity. Following Steps 1, 2 and 5, and using a free blog site, you can create a very powerful website to share your ideas.

These sites may not be sufficient for your needs, you may be risking a lack of control over the content once it is uploaded,

Step 3 - Anonymous Domain Name Registration

or you may be violating the terms of service by providing pseudonymous information and an anonymous email. For those who want to create a more robust website, you will need to get your own domain name.

To get a domain name, you need to register with a domain name registrar. Most registrars will ask for personally identifying information, in addition to collecting the IP address that was used, to register the domain. There are ways to register a domain while still protecting your identity.



ICANN is a private corporation which oversees all domain registration. The terms of service of that company require individuals to provide accurate personal information to register a domain name. Although they rarely verify the accuracy of the personal information provided, and the only penalty is cancellation of service, providing a pseudonym and inaccurate contact information directly to a domain registrar is not necessary to protect privacy.

Several companies will agree to provide accurate registration information without collecting your own personal

Step 3 - Anonymous Domain Name Registration

information, or allowing you to use pseudonymous information. This ensures that you are in compliance with all terms and conditions and are not at risk of losing your domain. Never providing your real identity to anyone is the only way to be sure to protect your privacy.

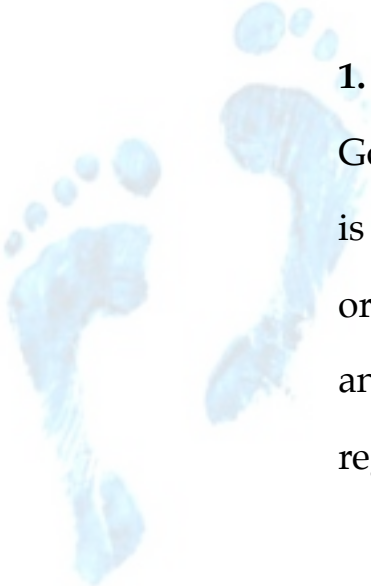
You need to provide a legitimate email address because most communication with your domain registrar will be by email. Use the anonymous email you set up in the previous step for anonymous communications. Regular mail will almost never be used for communications, so if you provide a pseudonymous mailing address, you will probably not miss any important information from your domain registrar.

Many domain registrars offer private registration options. As long as pseudonymous information can be given to the proxy for private registration without violating their terms of service, those options will be satisfactory.

As with any service provider, it is imperative to perform due diligence on the company before you use them to make sure they are legitimate.

Payment

Paying for any good or service, not just domain name registration, can create an audit trail that leads right back to you. Anytime you use Paypal, a credit card, a debit card, or a wire transfer, you are creating a record that identifies you. Criticizing powerful government or law enforcement officials who can circumvent due process, means corrupt officials can discover your identity, putting you at risk. There are a few ways to pay for domain name registration without revealing your identity.



1. Cash/Money Order – Some domain name registrars, like GoDaddy.com, accept money orders. Since domain registry is only a few dollars per year, it is very easy to pay by money order. Cash is another way to pay for any service anonymously, but it may be difficult to find a domain name registrar that accepts cash.

2. Prepaid Credit Card – Prepaid credit or debit cards are available in convenience stores and many other places and can be purchased with cash. They can be used to pay for a

Step 3 - Anonymous Domain Name Registration

domain name without being linked to your regular credit cards or bank account.

3. Bitcoin – [Bitcoin](#) is relatively anonymous. You can download the free software and use a wallet number that is completely unconnected to you. You can find someone in your town to buy Bitcoins for cash or buy them on an exchange. Some domain registrars accept payment in Bitcoins. Paying for your domain name in Bitcoins will eliminate identifying information. Since accepting Bitcoins is new among domain registrars, it is important to do thorough research before using them.

4. Offshore Domain Registrar – There are domain registrars in many countries. Critics of a government may find their personal and payment information more protected when using a domain registrar outside of their jurisdiction. Regimes change, politics shift and new alignments are made, so this may be the easiest but least secure of the anonymous options.

DOMAIN
REGISTRATION
RESOURCES

AnonymousSpeech.com

OrangeWebsite.com

Exoware.net

Shinjiru.com

NearlyFreeSpeech.net

PrivacyShark.com

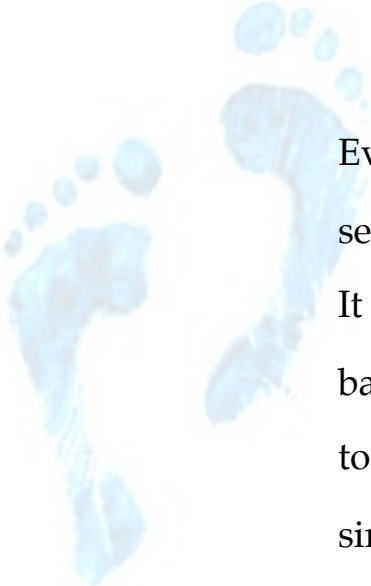
NameBay.com

[Free Website Builders](#)

“Protections for anonymous speech are vital to democratic discourse. Allowing dissenters to shield their identities frees them to express critical minority views . . . Anonymity is a shield from the tyranny of the majority. . . . It thus exemplifies the purpose behind the Bill of Rights and of the First Amendment in particular: to protect unpopular individuals from retaliation . . . at the hand of an intolerant society.”

McIntyre v. Ohio Elections Comm’n, 514 U.S. 334

Step 4 - Anonymous Web Hosting



Every website needs a server to host the website. The host server is the actual computer where your website is stored. It is also the computer you log into remotely to get into the back end of your website to upload content, make changes to the look of the website, manage comments, and other similar things.

Hosting your website on your own server is a mistake if you want to remain anonymous. Your server will have an IP

address that will in turn be linked to you. You could mitigate this risk by housing your server in a foreign country, but that will not be feasible for most people.

It is much more common for people to find a company that specializes in hosting websites. If you have used a free website provider, your hosting will be taken care of. If you are creating your own website, there are lots of web hosts to choose from, both domestically and abroad. Using a company to host your website introduces the payment problem again. How do you use a web hosting company when payment can be traced back to you?

There are some companies that will host websites for free. They usually force you to display ads on your website and may give you less control over it, so free hosting may not be for everyone.

Fortunately, there are plenty of web hosting companies that will host your website in exchange for cash, money order, prepaid credit cards or Bitcoins, much like domain name registrars. Most domain name registrars also offer web hosting, but there are many more web hosting companies

than there are domain registrars, so it should be easier to find a reputable web host which deals anonymously.

Don't forget to log into your website following the anonymous IP practices from Step 1 EVERY TIME, including the first time you sign up for web hosting.

HOSTING RESOURCES

WordPress.com (Free)

Blogsome.com (Free)

Yohost.org

Microtonix-Tech.com

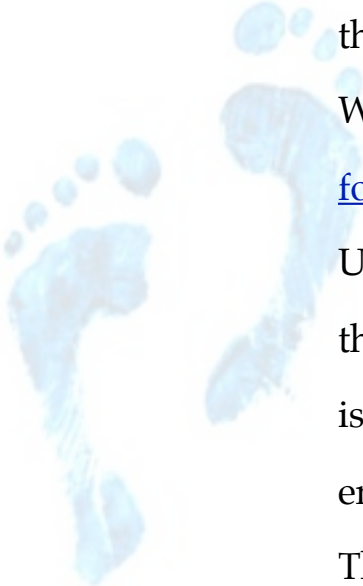
Invisihosting.com



“Free speech is the whole thing, the whole ball game. Free speech is life itself.”

Salman Rushdie

Step 5 - Anonymous Donations

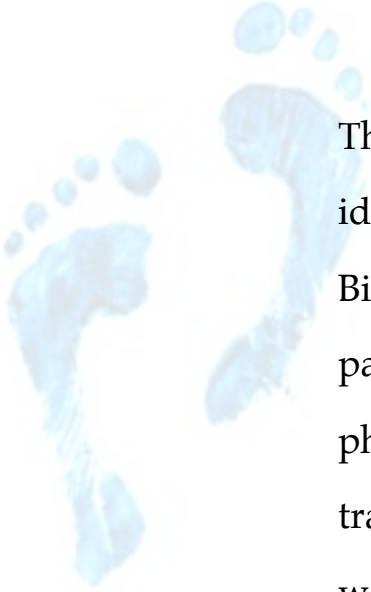


Many political activists look for donations to help support their cause or sell some items to help promote their message. Wikileaks suffered serious financial setbacks when the [formal banking system blockaded processing donations.](#) Using the formal financial system is one of the main ways that political activists can be identified. The financial system is also one of the best tools that corrupt politicians or law enforcement officials have to pressure political activists. There are several ways this pressure can be exerted.

Activists seeking donations sent to a particular bank account can be identified since banks must abide by know your

customer rules. Asking for checks made out to a certain name or entity is another way to identify the activist. Credit card payments to a certain person can be blocked, much like was done to Wikileaks.

One of the most anonymous and easiest ways to receive anonymous donations is with cash, gold or silver. Even with cash or bullion, you have to disclose an address where it can be sent. Any mailing address will probably have some connection to you, or to someone who knows your identity, which could compromise your identity, and lead to censorship, threats and violence.



The only way to receive donations without disclosing your identity and without being financially blockaded is by using Bitcoins. Unlike physical cash, gold or silver donations, the payments are sent over the internet. They require no physical address that can be linked to you. Bitcoins can be traded anywhere you have access to the internet, but your wallet will still be able to receive payments, whether you are connected to the internet or not. They are not bound by physical location or jurisdiction. They don't need identification and, unlike credit card, bank wires, Paypal or

Step 5 - Anonymous Donations

checks, Bitcoins cannot be frozen and payments cannot be blocked. Bitcoins, however, require some technical skill to use safely.



“Free speech is too dangerous to a democracy to be permitted.”

Henry Louis Mencken

Conclusion

This 5 step system for political activists is the perfect way to spread a politically sensitive message without facing censorship, threats or violence.

Step 1 – Protect your IP address every time you are working on your subversive website by using public Wi-Fi, Tor, or a VPN.

Step 2 – Get an anonymous email address.

Step 3 – Register your domain name offshore or under a pseudonym with a proxy using an anonymous form of payment.

Step 4 – Sign up for free web hosting or use an anonymous

form of payment.

Step 5 – Prepare yourself to accept donations in cash, gold, silver, or Bitcoins.

Unfortunately, too many people are forced to sacrifice their life, liberty or property in order to share their ideas. All it takes is a few simple steps for political activists and whistleblowers to protect their right to anonymous speech. It is up to you to follow them.





Copyright

HowToVanish.com
5 Steps To Anonymous Online Speech

© 2011, Bill Rounds, Esq.
HowToVanish.com

ALL RIGHTS RESERVED. This book contains material protected under International and Federal Copyright Laws and Treaties. Any unauthorized reprint or use of this material is prohibited. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system without express written permission from the author / publisher.