# BSD

## FOR NOVICE AND ADVANCED USERS

# Web Server Security

## RUNNING A WEB SERVER VIA RUMPRUN UNIKERNEL

## UNIX ACCESS CONTROL
## WITH SUDO

## REINSTALL
## AN OPENBSD 5.7 VPS
## WITHOUT KVM!

## AUGMENTED
## REALITY LAW,
## PRIVACY, AND ETHICS:

# FREENAS MINI
## STORAGE APPLIANCE

## IT *SAVES* YOUR LIFE.

## HOW IMPORTANT IS YOUR DATA?

Years of family photos. Your entire music and movie collection. Office documents you've put hours of work into. Backups for every computer you own. We ask again, *how important is your data?*

## NOW IMAGINE LOSING IT ALL

Losing one bit - that's all it takes. One single bit, and your file is gone.

The worst part? **You won't know until you absolutely need that file again.**

*Example of one-bit corruption*

## THE SOLUTION

The FreeNAS Mini has emerged as the clear choice to save your digital life. **No other NAS in its class offers ECC (error correcting code) memory and ZFS bitrot protection to ensure data always reaches disk without corruption and *never degrades over time*.**
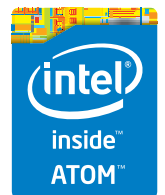
No other NAS combines the inherent data integrity and security of the ZFS filesystem with fast on-disk encryption. No other NAS provides comparable power and flexibility. The FreeNAS Mini is, hands-down, the best home and small office storage appliance you can buy on the market. **When it comes to saving your important data, there simply is no other solution.**

**The Mini boasts these state-of-the-art features:**

- 8-core 2.4GHz Intel® Atom™ processor
- Up to 16TB of storage capacity
- 16GB of ECC memory (with the option to upgrade to 32GB)
- 2 x 1 Gigabit network controllers
- Remote management port (IPMI)
- Tool-less design; hot swappable drive trays
- FreeNAS installed and configured

iXsystems ®

http://www.iXsystems.com/mini

intel inside™ ATOM™

Intel, the Intel logo, Intel Atom and Intel Atom Inside are trademarks of Intel Corporation in the U.S. and/or other countries.

# FREENAS CERTIFIED
## STORAGE



**With over six million downloads, FreeNAS is undisputedly *the* most popular storage operating system in the world.**

Sure, you could build your own FreeNAS system: research every hardware option, order all the parts, wait for everything to ship and arrive, vent at customer service because it *hasn't*, and finally build it yourself while hoping everything fits - only to install the software and discover that the system you spent *days* agonizing over **isn't even compatible**. Or...

## MAKE IT EASY ON YOURSELF

As the sponsors and lead developers of the FreeNAS project, iXsystems has combined over 20 years of hardware experience with our FreeNAS expertise to bring you FreeNAS Certified Storage. **We make it easy to enjoy all the benefits of FreeNAS without the headache of building, setting up, configuring, and supporting it yourself.** As one of the leaders in the storage industry, you know that you're getting the best combination of hardware designed for optimal performance with FreeNAS.

## Every FreeNAS server we ship is...

» Custom built and optimized for your use case
» Installed, configured, tested, and guaranteed to work out of the box
» Supported by the Silicon Valley team that designed and built it
» Backed by a 3 years parts and labor limited warranty

As one of the leaders in the storage industry, you know that you're getting the best combination of hardware designed for optimal performance with FreeNAS. **Contact us today for a FREE Risk Elimination Consultation with one of our FreeNAS experts.** Remember, every purchase directly supports the FreeNAS project so we can continue adding features and improvements to the software for years to come. **And really - why would you buy a FreeNAS server from *anyone* else?**
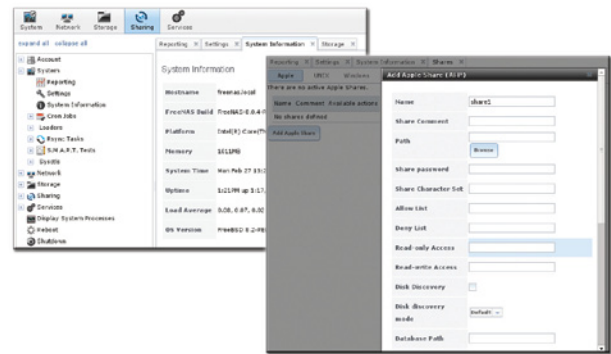


### FreeNAS 1U
• Intel® Xeon® Processor E3-1200v2 Family
• Up to 16TB of storage capacity
• 16GB ECC memory (upgradable to 32GB)
• 2 x 10/100/1000 Gigabit Ethernet controllers
• Redundant power supply

### FreeNAS 2U
• 2x Intel® Xeon® Processors E5-2600v2 Family
• Up to 48TB of storage capacity
• 32GB ECC memory (upgradable to 128GB)
• 4 x 1GbE Network interface (Onboard) - (Upgradable to 2 x 10 Gigabit Interface)
• Redundant Power Supply



**http://www.iXsystems.com/storage/freenas-certified-storage/**

## Dear Readers,

You are going to read the "Web Server Security" issue from BSD magazine. You will have the chance to learn how to run an application in a self contained environment that provides more security and, by removing the biggest parts of an operating system, consumes less space. What is more, our experts will discuss security related issues in sudo environments and evaluate advantages and disadvantages of centralizing sudo with LDAP back-end. Finally, you may find interest in this month's column provided by Rob Somerville about customer service, which is one of those disciplines that technologists, IT staff and certain sections of management generally baulk at. After all, we all have our own dragons to slay, so how can we peacefully co-exist with the suits that are determined to deliver excellence while policy dictates. More on the next pages. And … I would like to express my gratitude to our experts who contributed to this publication and invite others to cooperate with our magazine.

The next issue of BSD Magazine will be published in 4 weeks. If you are interested in learning more about the future content or you would like to get in touch with our team, please feel free to send your messages to ewa.d@bsdmag.org and I will be more than pleased to talk and answer all your questions.

Hope you enjoy the issue.

*Thank you.*
*Ewa & BSD Team*

# FreeNAS

## in an Enterprise Environment

By the time you're reading this, FreeNAS has been downloaded more than 5.5 million times. For home users, it's become an indispensable part of their daily lives, akin to the DVR. Meanwhile, all over the world, thousands of businesses universities, and government departments use FreeNAS to build effective storage solutions in myriad applications.

### What you will learn...

- How TrueNAS builds off the strong points of the FreeBSD and FreeNAS operating systems
- How TrueNAS meets modern storage challenges for enter~~~

The FreeNAS operating systems is fre~~~ the public and offers thorough doc~~~ active community, and a feature-ri~~~ the storage environment. Based on Free~~~ can share over a host of protocols (SM~~~ FTP, iSCSI, etc) and features an intuitiv~~~ the ZFS file system, a plug-in system ~~~ much more.

Despite the massive popularity ~~~ aren't aware of its big brother dut~~~ data in some of the most demand~~~ environments: the proven, enterp~~~ professionally-supported line of ~~~

But what makes TrueNAS diffe~~~ Well, I'm glad you asked...

### Commercial Grade Supp~~~

When a mission critical stor~~~ organization's whole operat~~~ halt. Whole community-bas~~~ free), it can't always get an~~~ and running in a timely m~~~ responsiveness and expe~~~ dedicated support team~~~ provide that safety.

Created by the sam~~~ developed FreeNAS.

# CONTENTS

# Dr.WEB® CureIt!™

# EMERGENCY CURING
## for Windows workstations and servers
including those running other anti-virus software

## FUNCTIONS:

- Cures Windows workstations and servers.
- Verifies the quality of the anti-virus software currently in use.

## FEATURES:

- Dr.Web CureIt! doesn't require installation and doesn't conflict with any known anti-virus; consequently there is no need to disable the anti-virus currently in use to check a system with Dr.Web CureIt!.
- Improved self-protection and an enhanced mode for more efficient countermeasures against Windows blockers.
- Dr.Web CureIt! is updated at least once an hour.
- The utility can be launched from removable media including USB storage devices.

## LICENSING FEATURES:

The utility is available for free when used for non-business purposes.

# Running a Web Server via Rumprun Unikernel

DAVID CARLIER

Running a web server in a usual monolithic operating system alongside with other services is the usual scenario. However, a web server can have many potential vectors of attacks, DDOS, SQL injections and so on ... hence threatening the host operating system. An alternative approach, called unikernel, allows you to run an application in a self contained environment that provides more security and, by removing the biggest parts of an operating system, consumes less space.

For our example, we'll use sthttpd (a fork of the former thttpd) and a Xen environment. And for producing an unikernel image, we'll use rumprun.

## Rumprun, building our software

Rumprun, which you can find in this repository *https://github.com/rumpkernel/rumprun*, provides a whole compilation toolchain, the NetBSD's libc and a couple of few libraries to run our software for Xen or qemu (with or without KVM) for example. The steps to make it workable are to compile the software (and eventually its dependencies) with the rumprun toolchain then make a unikernel image.

First we need to compile all the libraries needed to make unikernel images va the build-rr.sh shell script. This is pretty simple, we just need to type build-rr.sh `<platform where platform is xen or hw>`.

Note: If you wish to build both hw and xen versions, I suggest you compile in two separated git local clones rather than in one alone.

First we need the NetBSD source:

```
> git submodule update --init
> ./build-rr.sh xen
```

or if you have already the NetBSD source somewhere:

```
> ./build-rr.sh -s <path of NetBSD source> xen
```

After a couple of minutes, inside the app-tools subfolder, we should have our make, configure, linker, c and c++ ... and all other necessary wrappers. I'd suggest that you add your PATH environment to this app-tools folder.

Hence once inside sthttpd project folder, we can type

```
rumprun-xen-configure ./configure <your usual configure flags>
    which sets useful variables like CC/CXX ... host
> ac_cv_func_malloc_0_nonnull=yes rumprun-xen-configure ./
    configure
> rumprun-xen-make
```

```
> rumprun-xen-make install
```

We finally need to link our unikernel image (the application will be linked to rumpkernel libraries) via rumpbake script which can work only if the application was previously compiled via the rumprun toolchain. So we can type:

```
rumpbake <target> <unikernel image name> <executable>

> rumpbake xen_pv xen-thttpd <path to shttpd executable>
```

## Configuration

We will need to have available inside the Xen environment the web static content to serve and eventually the sthttpd configuration and a user/group database. Then we can make two isos archives via NetBSD mkisofs, Linux genisoimage ... one for the web content, we have already a www subfolder for it, and the other one for configuration purposes. Let's have an etc folder which contains the master.passwd/group file, pwd.db and spwd.db which contains a nobody user (directly grabbed from my NetBSD box) and a basic shttpd configuration file:

```
...
dir=/www
port=80
user=nobody
nochroot
...
```

## Launching the Xen instance and serving the content

Let's assume we already configured a minimal Xen bridge, in our case the Xen instance will have a dynamic IP address for the sake of simplicity. To launch our unikernel image, we will use the rumprun wrapper. We can type rumprun `<target> -n <network interface setting> -M <memory settings in MB> -b <block device 1>... -b<block device N> -di <path to the unikernel image> <arguments for the unikernel image>`

```
> rumprun xen -n inet,dhcp -M 128 -b etc.iso,/etc pb www.
  iso,/www -di xen-thttpd -D -C /etc/thttpd.conf
```

Note: If you are curious as to how Xen is launched, you can add the -D argument to rumprun which simply dumps the command in the standard output instead of launching it.

Now you should see, via xl list, your Xen instance named rumprun-xen-thttpd.

Normally, you can now see the web contents from your usual web browser ...

The unikernel approach is already used in production case, hence a well considered solution especially for better security and also if the service fails, the init process is faster. Hopefully, it will give you the curiosity at least to consider this approach in your own case.



**Figure 1.** *Working in progress*

# Best Practices in UNIX Access Control with SUDO

**LEONARDO NEVES BERNARDO**

This article will discuss about security related issues at sudo environments. Will be evaluated advantages and disadvantages of to centralize sudo with LDAP back-end. Another issue summarized in this article is about taking care with content of sudo registers.

In the early days of UNIX, there were only two kinds of users: administrators and common users. Until now, this structure remained in the same model. Nevertheless, in our day by day activity, it is very common to meet some situations where it is necessary to delegate some responsibilities to operational groups and the others, who are not administrators nor common users. Some administrators do some insecure techniques like: sharing of root passwords, creation of users with *uid 0*, changes in file permission, and so on. These techniques are a solution for the immediate problem, but don't follow least privilege principle.

Around 1972, the notable Dennis Ritchie invented the *setuid bit*. The setuid bit allows users to run an executable with the permissions of the executable's owner. The most common situation is when an executable is owned by root. Programs must be carefully designed when the *setuid* bit permission is enabled, because vulnerable applications allow an attacker to execute arbitrary code under the rights of the process being exploited. After *setuid* bit creation, the division between root and other users starts to be broken. Unfortunately, to take advantage of this feature, it is necessary to rewrite the programs.

Around 1980, Bob Coggeshall and Cliff Spencer wrote Substitute User DO, or SUDO, one *setuid* program to run other programs without the necessity of these programs being rewritten. *Sudo* became the most used tool for privilege escalation in the UNIX environment. *Sudo* is under constant development. Security concerns are very important in *sudo* and sometimes some vulnerabilities are discovered and corrected immediately.

## Basics about /etc/sudoers

The sudoers file is composed of three sections: defaults, aliases and user specifications.

## Defaults

Defaults defines options to be used in every *sudo* entry. It's possible to overwrite options in each entry. We will discuss a little about some options ahead in this article.

## Aliases

Aliases are variables used to group names. There are four types of aliases: `User_Alias`, `Runas_Alias`, `Host_Alias` and `Cmnd_Alias`. The name of an alias must start with an uppercase letter. Let's explain a little about each alias:

### User_Alias

Is used to define group of users, for example:

```
User_Alias   WEBMASTERS = user1, user2
```

You've probably realized UNIX has groups of users stored in the UNIX group of users (NSS group database) and

there is no needed to redefine those groups again. To use a UNIX group inside sudo, you need to append `%` in the register. In the following example, the UNIX group web-masters can be used inside sudoers as WEBMASTERS:

```
User_Alias    WEBMASTERS = %webmasters
```

### Runas_Alias
Is used to define group target users. Not always root is the target user, it's possible to use another users. x`Runas_Alias` is used to group them. Example:

```
Runas_Alias  OPERATORS = operator1, operator2
```

### Host_Alias
`/etc/sudoers` is prepared to be distributed among hosts. Hostnames, IP addresses and other kind of addresses are grouped in `Host_Alias`. Like `User_Alias`, it's possible to use a UNIX group of hosts, called netgroup (NSS net-group database). Netgroup is not very common, but is useful for big environments. To use UNIX netgroup inside *sudo*, you need to append `+` in the register. In the following example, a UNIX netgroup webservers can be used inside sudoers as WEBSERVERS:

```
Host_Alias    WEBSERVERS = +webservers
```

There are others possibilities to use `Host_Alias`, like lists of hostnames or ip addresses:

```
Host_Alias    WEBSERVER = host1, host2
Host_Alias    WEBSERVER = 192.168.0.1, 172.16.0.0/16
```

### Cmnd_Alias
`Cmnd_Alias` groups commands inside lists. Example of `Cmnd_Alias`:

```
CmnaAlias PRINTING= /usr/sbin/lpc, /usr/bin/lprm
```

For each one type of alias, there is one name built-in called ALL. It's possible to use *sudo* without any aliases, but aliases are recommended if you intend to use `/etc/sudoers`.

## User Specifications
In the end of the sudoers file, there are user specifications entries. The sudoers user specification is in following form:

```
user  host = (runas) command [,command,..]
user can be user, UNIX group prepending with % or User_Alias
host can be host, netgroup prepending with + or Host_Alias
runas can be user or group of user and unix group
```

command can be a command, list of commands divided by comma or Cmnd_Alias. command support wildcards.

Let's see an example of user specification:

```
root  ALL = (ALL) ALL
```

In the above example, it is shown one user entry which permits the root user to run all commands (last ALL), in all hosts (first ALL), becoming all users (ALL inside pa-renthesis) when running a command.

The following example is more restrictive than the first example:

```
neves  neves-laptop = (root) /usr/sbin/useradd
```

In this case, the user neves has permission to run the command `/usr/sbin/useradd` as user root in host neves-laptop only. As you can see, the second example is more adapted to the least privilege principle.

Let's go to see the result when user neves runs a com-mand directly:

```
$ /usr/sbin/useradd neves2
useradd: cannot lock /etc/passwd; try again later.
```

User neves doesn't have access to add user directly, but with sudo it could be possible:

```
$ sudo /usr/sbin/useradd neves2
[sudo] password for neves:
$
```

Well, it is a typical use of *sudo* and now it is possible to delegate some activities for operators group. By default, *sudo* requests the user password and maintains user password in cache for 5 minutes.

Let's see a little more complex example using aliases:

```
User_Alias    OPERATORS = neves, neves2
Host_Alias    DESKTOPS = neves-laptop, neves-laptop2
Cmnd_Alias    MNGUSERSCMDS = /usr/sbin/userdel, /usr/sbin/
    useradd, /usr/sbin/usermod
OPERATORS    DESKTOPS=(ALL)  MNGUSERSCMDS
```

Now, beyond `useradd` command, user neves is allowed to run `usermod` and `useradd` commands and sudoers is organized with aliases.

To manage `/etc/sudoers`, it is strongly recommended to use the `visudo` command. The advantage of the use of visudo is that it assures *sudo* syntax is correct before

allowing one to save the sudoers file. We've seen a little about file `/etc/sudoers`. Almost all environments use this way to control sudo and it is okay for standalone servers or small environments. We will see that file sudoers is not the best configuration for big and medium size networks.

## Common situations about sudoers distribution

Although it's possible to use `/etc/sudoers` setup in a per-host basis, sudo doesn't have any built-in way to distribute `/etc/sudoers` file among servers. It's very common in some companies that some team is in charge of operating and distributing `/etc/sudoers`. In another companies, there are scripts using version control (cvs, svn, etc), transfer commands (rsync, rdist, rcp, scp, ftp, wget, curl, etc.) or file share (nfs, netbios, etc.) to distribute `/etc/sudoers`. Although the use of scripts is better than manual operation, there are a lot of security issues to be considered in this case. There are some questions that need to be answered:

### Are Changes in /etc/sudoers audited?

Imagine one attacker using *sudo* to get root access in your environment. It's important to think about which information you have in your log when something like that happens.

### Do operators or scripts need root access to change /etc/sudoers?

If you are using push strategy to distribute `/etc/sudoers`, then probably the source will have rights to change destination servers, as the usual, with root access. In the worst case, with push strategy, you probably created one unique point where it is possible to get root access to entire environment.

### Is the source of /etc/sudoers trusted?

Instead push strategy, perhaps you are using pull strategy. In this case, all servers are getting `/etc/sudoers` from one central point. There are two major concerns in pull strategy, first it's necessary to protect from man in middle attacks and second is to raise security level of central point. In general, pull is the best strategy to deploy sudoers files, because security problems don't compromise the entire environment. If you use one software of configuration management like puppet or cfengine to distribute sudoers and protect the configuration management server, your environment probably has a reasonable level of security. Even so, the pull strategy with configuration management lacks real time updates and sometimes lacks an auditing of changes in sudoers files.

## Using back-end LDAP

Now let's discuss about the current best way to use *sudo*. With an LDAP back-end, *sudo* becomes a client-server service. For each use of *sudo*, the LDAP server will be consulted. We join the best advantages of LDAP and the best advantages of *sudo* to create one authorization system for UNIX environment.

### Advantages of LDAP

Some advantages to use LDAP as sudo back-end are:

- LDAP protocol is standards-based
- If well structured with replication servers, you will have a high availability service
- There are *access control lists* (ACLs)
- It's possible to audit all changes and all consults
- LDAP is cross-platform, it's possible even to change from one server to another completely different one (e.g.: from openldap to Microsoft active directory)
- LDAP is very fast for search operations (almost all commands in sudo service)
- It's possible to use cryptography/TLS as requirement

Beyond these advantages, maybe the most important security consideration is that it is not necessary to open some security breach to distribute the sudoers file.

I don't think it's necessary restate about the importance of protecting your LDAP server(s). Some basic actions like to use firewall, TLS and put LDAP servers in segregated network are outside the scope of this article. If you have a non protected LDAP environment, it is probably better to use another strategy.

### Creating LDAP structure

We will explain about how to build one basic LDAP server (OpenLDAP) to store *sudo* information. We will use OpenLDAP software, because OpenLDAP is the most widely known LDAP server distributed as open software. The procedures are about compilation of OpenLDAP, but if you prefer, you could install by package manager and achieve the same results. If you have one OpenLDAP server running, it is possible for you to jump to next topic. You could use another LDAP server instead openldap, but we won't explain about this, please look for information in *sudo* documentation.

First of all, download the latest release of the Berkeley DB from the Oracle site (*www.oracle.com/technetwork/ database/berkeleydb*) and latest version of OpenLDAP from the OpenLDAP site (*www.openldap.org*).

Compiling and installing Berkeley DB:

```
# tar -zxvf db-4.8.30.NC.tar.gz
# cd db-4.8.30.NC/build_unix/
# ../dist/configure && make && make install
```

OpenLDAP needs to find berkeley DB before compilation:

```
# export CFLAGS="-I/usr/local/BerkeleyDB.4.8/include"
# export CPPFLAGS="-I/usr/local/BerkeleyDB.4.8/include"
# export LDFLAGS="-L/usr/local/BerkeleyDB.4.8/lib"
# export LD_LIBRARY_PATH="/usr/local/BerkeleyDB.4.8/lib"
```

Compiling and installing OpenLDAP:

```
# tar -zxvf openldap-2.4.26.tgz
# cd openldap-2.4.26
# ./configure && make depend && make install
```

Let's start with a minimal OpenLDAP configuration file. Create a `/usr/local/etc/openldap/slapd.conf` with Listing 1 content.
   And finally, start LDAP server with the command:

```
# /usr/local/libexec/slapd
```

OpenLDAP will bind TCP port 389, verify with netstat command:

---

```
# netstat -an | grep 389
tcp     0   0 0.0.0.0:389        0.0.0.0:*     LISTEN
tcp6    0   0 :::389             :::*          LISTEN
```

The next step is to create the root of your LDAP tree. Create one file named *base.ldif* with Listing 2 content.
   And add content with the command ldapadd:

```
# ldapadd -D"cn=admin,dc=example,dc=com" -w"secret" -f
   base.ldif
adding new entry „dc=example,dc=com"
adding new entry „cn=admin,dc=example,dc=com"
```

Use ldapsearch to verify funcionality of your LDAP directory, as showed in Listing 3.
   If the results are like Listing 3, your OpenLDAP is okay. Remember that there are no security concerns in this server example. Your LDAP base is `dc=example,dc=com`, your admin user is `cn=admin,dc=example,dc=com` and your password of admin user is `secret`.

---

**Listing 1.** *Minimal slapd.conf*

```
#slapd.conf file
include          /usr/local/etc/openldap/schema/core.schema
pidfile          /usr/local/var/run/slapd.pid
argsfile         /usr/local/var/run/slapd.args

database         bdb
suffix           "dc=example,dc=com"
rootdn           "cn=admin,dc=example,dc=com"
rootpw           secret
directory        /var/lib/ldap
index    objectClass     eq
```

**Listing 2.** *Base ldif*

```
#base.ldif
dn: dc=example,dc=com
objectClass: dcObject
objectClass: organization
dc: example
o: example

dn: cn=admin,dc=example,dc=com
objectClass: organizationalRole
cn: admin
```

---

**Listing 3.** *Test with ldapsearch*

```
# ldapsearch -x -b "dc=example,dc=com" -LLL
dn: dc=example,dc=com
objectClass: dcObject
objectClass: organization
dc: example
o: example

dn: cn=admin,dc=example,dc=com
objectClass: organizationalRole
cn: admin
```

**Listing 4.** *Slapd.conf with sudo structure*

```
#slapd.conf file
include          /usr/local/etc/openldap/schema/core.schema
include          /usr/local/etc/openldap/schema/sudo.schema
pidfile          /usr/local/var/run/slapd.pid
argsfile         /usr/local/var/run/slapd.args

database         bdb
suffix           "dc=example,dc=com"
rootdn           "cn=admin,dc=example,dc=com"
rootpw           secret

index    objectClass     eq
index    sudoUser        eq
```

## Creating sudo container

Now it's necessary to prepare your OpenLDAP to accept sudo information. First step is to include the sudo.schema.

Download the latest stable *sudo* release source from the sudo site (*www.sudo.ws*) and copy the sudo.schema to the openldap schema directory:

```
# tar -zxvf sudo-1.8.2.tar.gz
# cp sudo-1.8.2/doc/schema.OpenLDAP /usr/local/etc/
    openldap/schema/sudo.schema
```

Edit slapd.conf to include the `sudo.schema` and index to sudoUser attribute. Listing 4 shows *slapd.conf* with information related to *sudo*. Restart slapd to reread the new configuration:

```
# killall slapd
# /usr/local/libexec/slapd
```

Create the file ldif *sudo* container, with the following content:

```
dn: ou=SUDOers,dc=example,dc=com
objectClass: top
objectClass: organizationalUnit
ou: SUDOers
```

Add to the directory with ldapadd:

```
# ldapadd -D"cn=admin,dc=example,dc=com" -w"secret" -f
    sudo.ldif
adding new entry „ou=SUDOers,dc=example,dc=com"
```

Your OpenLDAP is okay to control access with sudo. You have two possibilities at this moment, migrate your `/etc/sudoers` or start from zero.

## Migrating sudoers content

Usually the easiest way to migrate sudoers information to LDAP is using a script sudoers2ldif. sudoers2ldif is located at plugins/sudoers, from the *sudo* source. To generate ldif file from `/etc/sudoers`, use the following commands:

```
# SUDOERS_BASE=ou=SUDOers,dc=example,dc=com
# export SUDOERS_BASE
# /usr/src/sudo-1.8.2/plugins/sudoers/sudoers2ldif /etc/
    sudoers > sudoers.ldif
```

And importing *sudoers.ldif* content to LDAP server:

```
# ldapadd -D"cn=admin,dc=example,dc=com" -w"secret" -f
    sudoers.ldif
```

```
adding new entry „cn=defaults,ou=SUDOers,dc=example,dc=com"

adding new entry „cn=root,ou=SUDOers,dc=example,dc=com"

adding new entry „cn=OPERATORS,ou=SUDOers,dc=example,dc=com"
```

The script sudoers2ldif creates one register called defaults containing the default options and creating one LDAP register for each `/etc/sudoers` entry. Sometimes it's necessary to correct resulting ldif file before importing to LDAP. It happens because, depending your sudoers file, it sometimes creates more than one LDAP entry with the same DN (distinguished name). Duplicate DNs aren't supported by LDAP protocol.

## LDAP sudoers registers

First, the difference between `/etc/sudoers` and sudoers inside LDAP is that, inside LDAP there are no aliases.

First of all, sudo looks for the register `cn=defaults` and parses it like a Defaults section in `/etc/sudoers`. The cn=defaults is a list of `sudoOptions`.

Other *sudo* registers, in general, are formed by combination of attributes `sudoHost`, `sudoUser` and

**Listing 5.** *sudo LDAP entry*

```
# OPERATORS, SUDOers, example.com
dn: cn=OPERATORS,ou=SUDOers,dc=example,dc=com
objectClass: top
objectClass: sudoRole
cn: OPERATORS
sudoUser: neves
sudoUser: neves2
sudoHost: neves-laptop
sudoHost: neves-laptop2
sudoRunAsUser: ALL
sudoCommand: /usr/sbin/userdel
sudoCommand: /usr/sbin/useradd
sudoCommand: /usr/sbin/usermod
```

**Listing 6.** *ldap.conf with sudo*

```
base dc=example,dc=com
uri ldap://localhost/
ldap_version 3
SUDOERS_BASE ou=SUDOers,dc=example,dc=com
SUDOERS_DEBUG 1

Modify /etc/nsswitch.conf and add sudoers backend:
sudoers:    ldap
```

**Listing 7.** *Testing sudo with LDAP*

```
$ sudo /usr/sbin/useradd neves2
LDAP Config Summary
===================
uri            ldap://localhost/
ldap_version 3
sudoers_base ou=SUDOers,dc=example,dc=com
binddn         (anonymous)
bindpw         (anonymous)
ssl            (no)
===================
sudo: ldap_initialize(ld, ldap://localhost/)
sudo: ldap_set_option: debug -> 0
sudo: ldap_set_option: ldap_version -> 3
sudo: ldap_sasl_bind_s() ok
sudo: Looking for cn=defaults: cn=defaults
sudo: found:cn=defaults,ou=SUDOers,dc=example,dc=com
sudo: ldap sudoOption: 'env_reset'
sudo: ldap search '(|(sudoUser=neves)(sudoUser=%neves)
   (sudoUser=ALL))'
sudo: searching from base
   'ou=SUDOers,dc=example,dc=com'

sudo: ldap sudoHost 'neves-laptop' ... MATCH!
sudo: order attribute raw: 3
sudo: order attribute: 3.000000
sudo: result now has 1 entries
sudo: ldap search '(sudoUser=+*)'
sudo: searching from base
   'ou=SUDOers,dc=example,dc=com'
sudo: adding search result
sudo: result now has 1 entries
sudo: sorting remaining 1 entries
sudo: searching LDAP for sudoers entries
sudo: ldap sudoRunAsUser 'ALL' ... MATCH!
sudo: ldap sudoCommand '/usr/sbin/userdel' ... not
sudo: ldap sudoCommand '/usr/sbin/useradd' ... MATCH!
sudo: ldap sudoCommand '/usr/sbin/usermod' ... MATCH!
sudo: Command allowed
sudo: LDAP entry: 0x1f90790
sudo: done with LDAP searches
sudo: user_matches=1
sudo: host_matches=1
sudo: sudo_ldap_lookup(0)=0x02
Password:
sudo: removing reusable search result
neves@neves-laptop:~$
```

sudoCommand. It's possible to use multiple values in each these attributes.

Listing 5 shows one example of sudo LDAP entry. In Listing 5, there is a sudo LDAP register with multiples of sudoUser, multiples of sudoHost and multiples of sudoCommand. It's possible to use attributes sudoRunAs, sudoOption, sudoRunAsUser, sudoRunAsGroup, sudoNotBefore, sudoNotAfter, sudoOrder, sudoNotBefore and sudoNotAfter are very interesting, because it's possible to define the time that permission is valid in sudo.

### Compiling and configuring sudoers LDAP client

Above 1.6.8 version of sudo, LDAP support is available. Some linux distributions, like Red Hat now distribute software packages of *sudo* with LDAP support, but in general, some Unix vendors and linux distributions distribute *sudo* without LDAP support.

Let's see how to compile *sudo* with LDAP and NSS (Name Service Switch). With NSS, sudo will be one of NSS databases, like passwd or group. If your UNIX doesn't have NSS support, it's possible to use LDAP support inside *sudo*, but you need to look at your operating system documentation to learn how to use LDAP back-ends in authentication.

Download, uncompress and install sudo with LDAP support:

```
# tar -zxvf sudo-1.8.2.tar.gz
# cd sudo-1.8.2
# ./configure --with-ldap && make && make install
```

Edit your /etc/ldap.conf using Listing 6 as reference. We will enable SUDOERS_DEBUG to confirm that our sudo binary is using LDAP back-end.

And let's test the configuration, as showed in Listing 7.

In Listing 7, we've seen that sudo consulted LDAP to get information about authorization. Look at line:

```
sudo: ldap search '(|(sudoUser=neves)(sudoUser=%neves)
   (sudoUser=ALL))'
Sudo looks for user, ALL and all groups of user using
   charactere '%'
```

Don't forget to remove the SUDOERS_DEBUG line from /etc/ldap.conf. It's recommended to remove the old sudo binary (usually /usr/bin/sudo) and the old /etc/sudoers file.

### Using groups and netgroups to organize sudo registers

There are no aliases in *sudo* when we are using LDAP. Aliases are useful to organize registers and avoid operation confusion. It's possible to implement the same

aliases functionality in NSS aware operating systems to `User_Alias` and to `Host_Alias`. Unfortunately, it's not possible to use command aliases (`Cmnd_Alias`).

The idea is to create a group container inside LDAP to store sudo groups like `User_Alias`. These groups will visible to whole environment. Sometimes your environment is LDAP aware and next steps could be already done.

Extend your slapd.conf to include following schemas:

```
include        /usr/local/etc/openldap/schema/cosine.schema
include     /usr/local/etc/openldap/schema/inetorgperson.schema
include     /usr/local/etc/openldap/schema/nis.schema
```

### Create ldif file to group container with the content:

```
cn: ou=group,dc=example,dc=com
objectclass:organizationalunit
ou: groupd
```

### Import to LDAP:

```
# ldapadd -x -h localhost -D"cn=admin,dc=example,dc=com"
   -w secret -f groups.ldif
adding new entry „ou=group,dc=example,dc=com"
```

### Create a ldif file with your group. Take care about the gidNumber, because the gidNumber mustn't conflict with local gid numbers:

```
dn: cn=sudooperators,ou=Group,dc=example,dc=com
objectClass: top
objectClass: posixGroup
cn: sudooperators
gidNumber: 3000
```

### Import to ldap:

```
# ldapadd -D"cn=admin,dc=example,dc=com" -w"secret" -f
   sudooperators.ldif

adding new entry „cn=sudooperators,ou=group,dc=example,dc
   =com"
```

### Configure your `/etc/ldap.conf` to add NSS group database:

```
nss_base_group  ou=Group,dc=example,dc=com
```

### Configure your `/etc/nsswitch.conf` to include ldap backend in group database, changing line starting with group to:

```
group compat ldap
```

Now, sudo groups inside LDAP are ready to be used inside the sudo register. Use sudoUser in the following format:

```
sudoUser: %group
```

The next step is to prepare a netgroup container. Netgroup is a part of NIS and NIS is an old software used to centralize network information. It is more often recommended to use LDAP instead NIS. Create a file named netgroup.ldif with the following content:

```
dn: ou=netgroup,dc=example,dc=com
objectClass: organizationalUnit
ou: netgroup
```

### And import to directory:

```
# ldapadd -D"cn=admin,dc=example,dc=com" -w"secret" -f
   netgroup.ldif
adding new entry „ou=netgroup,dc=example,dc=com"
```

### Create a netgroup ldif file with content like Listing 8. Import to LDAP:

```
# ldapadd -D"cn=admin,dc=example,dc=com" -w"secret" -f
   desktops.ldif
adding new entry „cn=desktops,ou=netgroup,dc=example,dc=com"
```

---

**Listing 8.** *netgroup example ldif file*

```
dn: cn=desktops,ou=netgroup,dc=example,dc=com
objectClass: nisNetgroup
objectClass: top
cn: desktops
nisNetgroupTriple: (neves-desktop,,)
nisNetgroupTriple: (neves-desktop2,,)
```

**Listing 9.** *Sudo LDAP register with LDAP groups and netgroups*

```
dn: cn=desktops_sudooperators,ou=SUDOers,dc=example,d
   c=com
objectClass: top
objectClass: sudoRole
cn: desktops_sudooperators
sudoCommand: /usr/sbin/userdel
sudoCommand: /usr/sbin/useradd
sudoCommand: /usr/sbin/usermod
sudoHost: +desktops
sudoUser: %sudooperators
```

The `nisNetgroupTriple` has 3 fields, host, user and domain. Even though it's possible to use these 3 fields in *sudo* directly, it's more recommended use NSS groups and use only first field of `nisNetgroupTriple` to store the names of computers. It's necessary to maintain the format with parenthesis and divided by commas `(,,)`.

Configure your `/etc/ldap.conf` to add NSS netgroup database:

```
nss_base_group  ou=Group,dc=example,dc=com
```

And configure your `/etc/nsswitch.conf` to include the ldap backend in the group database by changing the line started by group to:

```
group compat ldap
```

Finally, it's possible to change `sudoHost` to following format:

```
sudoHost: %netgroup
```

Listing 9 shows a complete sudo register with sudoGroup and sudoHost using LDAP groups and netgroups in ldif format. Even though it's possible to use netgroups inside `/etc/netgroups` and groups inside `/etc/groups`, useing LDAP as a back-end is more powerful because of centralized control. I recommend using groups and netgroups always and avoiding the use of multiples of sudoUser or sudoHost in the sudo register. This way, you will avoid confusion and will have the sudo structure standardized.

## Protect sudo registers
### Option noexec
Inside some Unix commands, it's possible to run other Unix commands. Examples of this are editors vi and vim and the find tool. With vi and vim it's possible to run commands using `:!`. Putting vi inside sudo is like putting bash or ALL, because one user executes `:!bash` and has a entire control of operation system, running commands with super user powers. Another example is the find tool with exec action. Imagine one user with the find tool, using the following command:

```
# sudo find /etc/ -exec chmod o+rwx {} \;
```

Probably, if you are responsible for this operating system, you would be in trouble.

Sudo has a option to prevent this kind of security problem through named noexec. With noexec, if your operating system supports `LD_PRELOAD`, sudo will prevent the execution of another command. Running sudo vim, and

after that vim command `:!bash`, for example, will show the following message error:

```
"Cannot execute shell /bin/bash"
```

Even though noexec is effective for many security problems related to sudo, it sometimes is useless. In the above example, we control the possibility of a normal user to getting a shell with super user power inside vim, but imagine if the same user runs vim by sudo and after that the user opens `/etc/passwd` and change uid for himself to 0. Whether the operating system doesn't have `LD_PRELOAD` support or binary is compiled statically, the no-exec feature of sudo won't work. Fortunately all modern flavors of Unix have `LD_PRELOAD` support. If you control binaries of the operating system with file integrity software like tripwire, samhain or aide, concerns about binaries statically compiled are reduced. I recommend you to use `sudoOption: noexec in cn=defaults`.

### Take care about variables
*Sudo* has some options like `env_reset`, `env_keep` and env_ check to control which environment variables will be available to use by commands called by sudo. It's very important to watch how the variables are interpreted by the destination command to avoid some security holes. In general, use `env_reset` enabled in `cn=default`. With this, only a few variables will be available in destination command.

### Use valid commands
Put in *sudo* only valid commands, in preference with absolute path. If you use *sudo* registers to some command which doesn't exists, if one user gets root access in that moment, he can install his own binary in the path appointed by `sudoCommand`. After that, this user will get root access by *sudo* every time without your knowledge. Beyond cares about valid commands in `sudoCommand`, it's highly recommended to complement with a file integrity software like tripwire or aide.

**ABOUT THE AUTHOR**

*Leonardo Neves Bernardo got started with Unix in 1996 when considered this operating system more interesting than any other. For more than fifteen years he worked with several IT area and now he is more focused with IT security area. Leonardo is LPIC-3, LPIC-302 and LPIC-303 certified and hold a Bachelor's degree in Computer Science from Universidade Federal de Santa Catarina, Florianópolis, Santa Catarina Brazil as well as RHCT and ITILv3 Foundation certifications. Visit his linkedin profile at: www.linkedin.com/profile/view?id=24995684*

# OpenBSD 5.7

## Reinstall OpenBSD 5.7 automatically, perfect for VPS! You don't need a KVM!
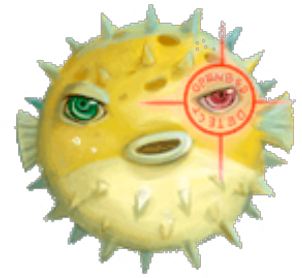
**WESLEY MOUEDINE ASSABY**

## What do you need?

- A running OpenBSD 5.7 system
- The source files: sys.tar.gz (kernel) & src.tar.gz (userland) to compile the new ramdisk kernel: bsd.rd
- Internet connection

Please, first read the man pages: autoinstall(8) and *don't forget to make a backup before!*

## Step 1
Get the source files and extract them

```
cd /tmp
ftp http://ftp2.fr.openbsd.org/pub/OpenBSD/5.7/src.tar.gz
ftp http://ftp2.fr.openbsd.org/pub/OpenBSD/5.7/sys.tar.gz
tar zxf src.tar.gz -C /usr/src
tar zxf sys.tar.gz -C /usr/src
```

## Step 2
Create the answer file auto_install.conf, and modify at your convenience

```
touch /usr/src/distrib/miniroot/auto_install.conf
```

Here's a sample:

```
Choose your keyboard layout = fr
System hostname = obsd
Password for root account = YOUR_PASSWORD_HASH
Start ntpd(8) by default = y
What timezone are you in = Indian/Reunion
Location of sets = http
HTTP Server = ftp2.fr.openbsd.org
Set name(s) = -g* -x* +xb*
```

Generate hash for password:

```
encrypt -b 8
```

## Step 3
Add the following line to the file `/usr/src/distrib/$(machine)/common/list`:

```
COPY  ${CURDIR}/../../miniroot/auto_install.conf
   auto_install.conf
```

## Step 4
Compile

```
cd /usr/src/distrib/special
make clean
make obj
make
make install

cd /usr/src/distrib/$(machine)
make clean
make obj
make depend
make
```

## Step 5
Install the new ramdisk kernel

```
cd /usr/src/distrib/$(machine)/ramdisk_cd/obj/
cp bsd.rd /
echo „boot bsd.rd" >> /etc/boot.conf
reboot
```

Enjoy, you will have now a new fresh OpenBSD installed!

**ABOUT THE AUTHOR**

*Wesley Mouedine Assaby lives in Reunion island, near Mauritius, works as network administrator at AISE-INFORMATIQUE (http://www.aise.re) where he installs some firewalls (Soekris appliances), mail server, all using OpenBSD system. He used it since 2007.*
*contact: wesley [at] mouedine [dot] net*

Attend

# InterDrone

## The International Drone Conference and Exposition

## InterDrone is Three Awesome Conferences:

### Drone TECHCON

**For Builders**

More than 35 classes, tutorials and panels for hardware and embedded engineers, designers and software developers building commercial drones and the software that controls them.

### Drone FLYER

**For Flyers and Buyers**

More than 35 tutorials and classes on drone operations, flying tips and tricks, range, navigation, payloads, stability, avoiding crashes, power, environmental considerations, which drone is for you, and more!

### Drone BUSINESS

**For Business Owners, Entrepreneurs & Dealers**

Classes will focus on running a drone business, the latest FAA requirements and restrictions, supporting and educating drone buyers, marketing drone services, and where the next hot opportunities are likely to be!

The Largest Commercial Drone Show in North America

*Meet with 80+ exhibitors!*
*Demos! Panels! Keynotes!*
*The Zipline!*

**September 9-10-11, 2015**
**Rio, Las Vegas**

www.InterDrone.com

A BZ Media Event

# RDS1025 Wave Rambler USB Pen PC Oscilloscope from Sain Smart

**REVIEWED BY BOB MONROE**

There is an old business motto that says "If you can't measure it, you can't manage it." Of course this is baloney because intangibles like your reputation, trust, credibility and validity are manageable in almost all forms. Most of those qualities you should manage or else find a new job as a politician. An oscilloscope is a measurement tool, sort of like a multimeter or voltmeter on steroids. This sky blue pen oscilloscope measures current, amps, and voltage as well as sampling rates of 100 milliseconds. The timing rate isn't huge but it's certainly good enough for most diagnostics and troubleshooting procedures. To obtain this timing rate, you must use the particular USB cable that comes with the device. That USB cable is a bit thick but is designed for these oscilloscope specifications.

The device is boxed up quite well but I had a heck of a time locating the installation CD. There isn't one. Instead Sain Smart provides a USB thumb drive with all the necessary files and documentation. Even the most expensive computers don't come with this great tool. I was impressed at this idea of forgoing the CD or having the new owner downloading the software from a site. A label on the USB stick would have been a really cool addition but a magic marker works just as well.

The only recommendation I would suggest is the addition of an internal lithium ion battery. The pen is tethered to your computer by a USB 2.0 cable, which provides the power and the input data for the electrical component being tested. So my recommendation for an internal battery is due to my own laziness and nothing else. I like portability and adding a battery would then have me asking for a memory card like a microSD for measurement logging (which is already done by the connected computer). After those requests were filled, I'd keep asking for more and more features, like an additional probe, a sandwich and a 3D printer for my birthday. Some folks have asked for WiFi or Bluetooth connectivity instead of USB but that could interfere with the sensors (EMI). You just can't please everyone. The pen oscilloscope is exactly the size you would think it would be; the size of a multi-colored ink pen. The Wave Rambler VPO 1025 sits in your pocket and it's up to you to figure out which pointy end you want facing which direction. The design has a clip like almost all pens do to keep the $96.99 device from falling out of your shirt or pant pockets. Don't try to write with it, though. Bad idea. Also, even though the oscilloscope is capable of testing to this range don't try to probe anything running 1,000 volts. Yes, it's not the volts that kill you it's the amps but why put the floating measurement (isolation voltage) to that kind of test when it is really rated at a maximum of 400Vs for the "I" version. Even that is pretty high for the size of this cool little device. This tool was built with ergonomics in mind because it fits comfortably in the hand for long periods of time. You have to try out the small trackball mounted on the top of the pen in exactly the same spot you would place your index finger. If you've ever used a drawing tablet then you should feel right at home using the trackball on this pen. There is a slide switch so you can change out probes depending on your testing and the package includes an additional hook probe connection. Don't expect lots of printed documentation with the Sain Smart VPO 10125. You can find all the details you would ever want at: *http://www.sainsmart.com/tools-equipments/oscilloscope-dso/sainsmart-vpo1025-pen-type-handheld-oscilloscope-25mhz-100ms-s-usb-dso.html*. The included USB stick has the most current driver and software for the pen oscilloscope so don't worry too much

about the software link at the bottom of the web page listed here. I did run into a few issues installing the Sain Smart software but that was because of all the security tools I have running on my machines. You shouldn't have any problems unless you are running HIDS, which if you don't know what HIDS is then you probably aren't running it.

The measurements were crisp and accurate during my testing of the Wave Rambler 1025. Basically, the pen is the probe and all the measurements are gathered and displayed on your USB connected computer. It didn't seem to matter if I was using USB 3.0 (blue connection) or 2.0. It did matter quite a bit when I decided to test the pen using a spare microUSB to USB cable. The Sain Smart device knew right away that the cable was incorrect and asked me to check my connection. Being the tester I am, I didn't change the connection and being the good product it was, it didn't allow it to connect with the improper cable.

Sain Smart put plenty of thought into the PC Oscilloscope VPO software. The opening screen shows the user tips on how everything works and can be used. The pen operation itself is fairly straightforward since there aren't too many ways to mess up the probe selection switch, the trackball or the user defined Z button. I haven't figured out how to get the customizable Z button to make me a sandwich (it's a hardware issue, I guess).

I enjoyed the screen showing me measurements as well as locations of where those measurements were taken. This gave me a visual representation of how the circuits worked based on where each probe touched. Being a visual person, this really helped me out when I was troubleshooting a TFT screen that had a bad HDMI output from the power management chip. I was able to see where the signal started and where it stopped along with the intermittent power changes that might have been impossible to detect using a traditional multimeter.

A little bit of solder and my TFT screen was fixed. It took me longer to set up my solder station than it did to test the board and locate the fault. That saved me $45 in under 15 minutes. I would be interested in porting the Sain Smart software over to a microcomputer like the Raspberry Pi. That would give me even greater flexibility for those odd jobs that need a quick diagnostic tool to repair the damaged circuit.

From my vantage point, I see great potential for the Sain Smart Wave Rambler 1025 pen oscilloscope. At under $100, this tool will pay for itself in a few projects. Anyone working on microcomputers, circuits, radios or pretty much anything besides a puppy or a sandwich will need such a device. As the Internet of Things (IoT) becomes more of a daily reality, fixing your own gadgets will require more sophisticated tools like a pen oscilloscope instead of a hammer and a screwdriver.

# Why ZIL Size Matters (or Doesn't)

**MARTY GODSEY**

Years of photos, audio, and video – we make True-eNAS because data is critical. Storage downtime can equal an instant loss of revenue. TrueNAS eliminates the RAID hardware used in traditional storage and replaces it with ZFS which combines the roles of RAID controller, Volume Manager, and File System. In the world of ZFS, we all know that RAM size is king. We spent over 2 years building TrueNAS, including selecting the RAM size for each TrueNAS model, so we are experts in how ZFS uses RAM.
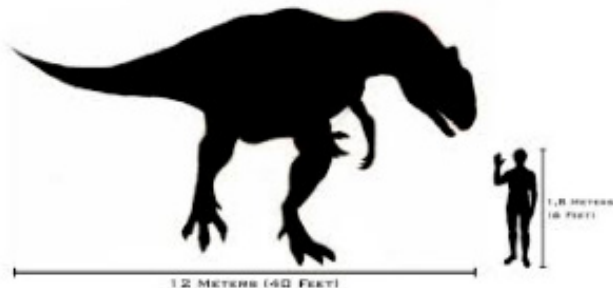


Many applications require more writes than reads, so customers want to know how to tune ZFS for their requirements. I let them know that ZFS requires little tuning and TrueNAS requires even less. This is because TrueNAS uses TrueCache™ and places fast, non-volatile read and write caches in front of the disks. Customers then say, "I use FreeNAS, not TrueNAS. What about me?" ZFS loves RAM and uses it for many things. It is used for read caching of the „hot data" set for your filer as well as metadata and L2ARC reference data, and other items. But increasing RAM is not the solution to improving write performance – use a ZFS "separate intent log" (SLOG) device instead!

TrueNAS uses a SLOG that has non-volatile RAM as a write-cache. It's easier to refer to this as the ZIL, but that is not totally accurate. ZFS always has a ZIL or „ZFS Intent Log". However if you don't have a SLOG, it is stored on the hard disk and your writes get hard disk performance. Depending on your level of protection (RAID-Z1, RAID-Z2, etc), this may be slower than you expect. For example, if you use RAID-Z2, each write will be performed 6 times. You paid for 144 IOPS out of your hard disk, but you only get 24.

| Protection Type | Writes Required |
| --- | --- |
| RAID-Z1 | 4 |
| RAID-Z2 | 6 |
| RAID-Z3 | 8 |
| RAID-10 | 2 |

Now you know why TrueNAS uses a SLOG. It uses a SLOG to commit the writes when they hit the cache and not worry about the hard disk IOPS. This enables the application to think it's been written to disk and continue with additional write operations. A question that often comes up is: How much space do I need? Do I need an expensive SLC SSD that stores hundreds of gigs for my SLOG or can I use a much smaller and cheaper SSD? The answer is yes, you can. The SLOG is very specific in how it functions, so you only have to worry about one specific aspect of your IO: write performance. And to even take this a step further: synchronous writes. Now you're saying: how in the world do I determine this? There are some guidelines you can use if you are building a filer for hundreds or thousands of users or for an extremely busy database application, but I'm going to give guidance for the other 95%+ of you. ZFS will take data written to the ZIL and write it to your pool every 5 seconds. Here is some simple throughput math using a 1Gb connection. The maximum throughput, ignoring overheads and assuming one direction, would be .125 Gigabytes per second. With 5 seconds between SLOG flushes and using a 1Gbit link with 100% synchronous writes, the most you will see written to your SLOG is 5 x .125 GB = .625 GB.

This shows that you don't need that much space for a SLOG and can use a smaller SSD. If you have a write-intensive application that requires multiple 1Gb Ethernet connects or a 10Gb, you can increase the size proportionally. So bringing it home – when choosing an SSD for a SLOG device, don't worry about space. Choose an SSD device that has extremely low latency, a high write IOPS, and is reliable. iXsystems did so for TrueNAS and the FreeNAS Mini and so should you.

## ABOUT THE AUTHOR

*Marty Godsey IXsystems Company (http://www.ixsystems.com/), Sales Engineer.*
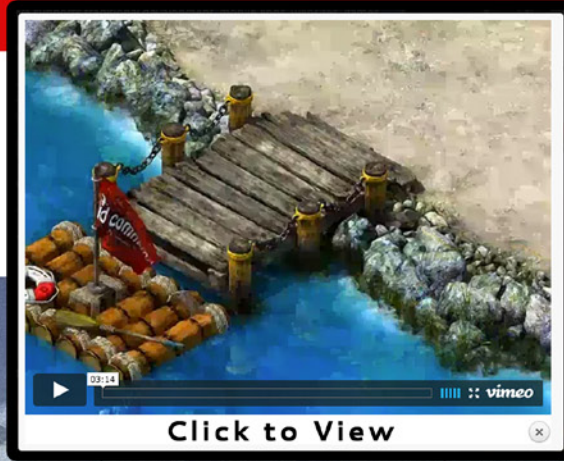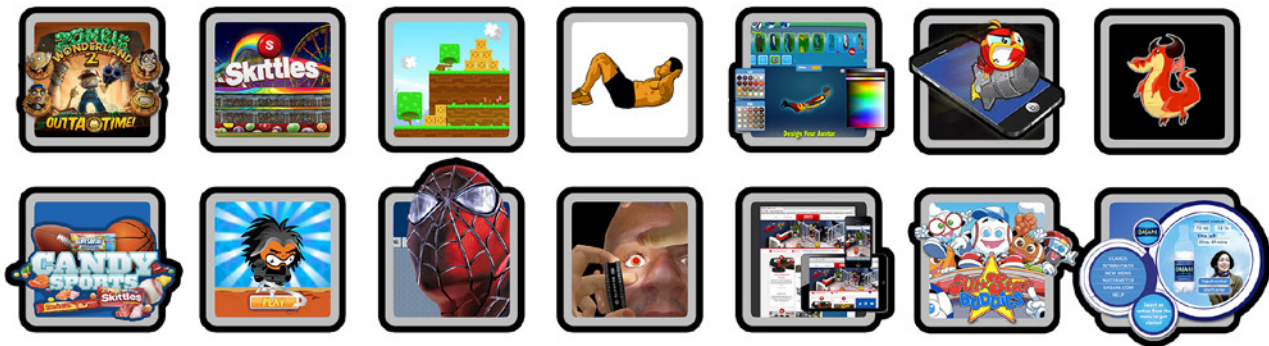
# Customer service – like opposing poles of magnets – is one of these disciplines that technologists, IT staff and certain sections of management generally baulk at. After all, we all have our own dragons to slay, so how can we peacefully co-exist with the suits that are determined to deliver excellence while policy dictates "expectations management" and "cost control"?

ROB SOMERVILLE

Having worked as a support engineer, in my experience both providing and receiving excellent customer support is an integral part of the role. Traditionally, the support model is based around a 3 or 4 tiered system, with level 1 dealing with the general day to day issues like password resets and software upgrades, up to level 4 where external suppliers like hardware vendors or 3rd party software suppliers are consulted. This model works on a ‚need to know' basis, and correspondingly often the level of autonomy and experience decreases the further down the chain. Naturally, the policy of most organisations is that the customer has to start at the lowest level, but unless sufficient care has been taken to leverage the knowledge base and customer history (e.g. via a CRM for instance) customer satisfaction and goodwill can rapidly deteriorate as they have to jump through the same hoops time and time again as the problem is escalated. There is also the issue of corporate culture as well to consider; unless the organisation completely embraces the concept that the customer – not the shareholders – pays their wages, there will always be the spectre of poor or even unethical customer service as ultimately profit or perceived loss will be the deciding factor.

The classic example of this was the issue in the 1970's where the Ford Motor Company in a fit of corporate blindness amidst a race to head off increasing pressure from Japanese imports, made the decision on the basis of cost-benefit reasoning not to upgrade the fuel tank of the Pinto. This resulted in a number of fatalities due to rear-end impacts and little was done to address this injustice as the cost of a product recall far outweighed any insurance claims. The number of victims of this cynical decision range between 23 and almost 500 depending who you ask. While in human terms the cost is immeasurable, the damage to the Ford Motor Company still lingers in popular culture, as an oblique reference of the main character in the movie Fight Club attests.

Rarely will customer service involve life and death decisions, unless the supplier is in a particularly sensitive sector such as pharmaceuticals, civil or building engineering or health care. There are those that would argue that ethically and materially the quality of the product is as far detached from customer service as the moon is from planet earth. This stance ignores the relationship between brand and reputation management – and as any marketing man-

ager worth their salt will tell you it is a) almost impossible to turn around a dissatisfied customer, b) bad news always travels faster than good and c) it is so much easier to sell to existing customers than generate new ones. In the Internet age, any customer looking for good value will research a company and their product prior to purchase, even if it is just reviewing the comments on Amazon.com. So in theory, customer service should be improving. That is, until the spectre of expectations management raises it's ugly head and rather than a brick wall of policy (The organisation says "No") a more subtle form of manipulation is exerted.

Expectations management has its roots in metrics, and the core philosophy is if you keep the customer informed, explain clearly what is and is not available (Deliverables), the customer will be satisfied even if you say no, as the parameters are already defined in a softer format than the hard hitting service level agreement beneath. Like the velvet glove surrounding the iron fist, expectations management can only absorb so many of the tears of the dissatisfied customer, until frustration, anger then rebellion and disillusionment set in. As a management strategy it performs well to stave off the enemy at the pass, allowing a "tick-box exercise" mentality to flourish amongst the counters of beans who have little respect for anything that doesn't fit. And before I have an army of accountants descent upon me in wrath, this particular mentality now extends to project managers and decisions makers at many levels as the curse of statistics and the subtle evil of inaccurate measurement seduces all.

I am long enough in the tooth to remember the issues in the 1970's that brought Ford to the point of despair with the Pinto – the foreign import. Supported by a weak currency, low employment costs and an insatiable drive to capture Western markets the Far East had a field day until it hit the buffers – quality. Ford management was spooked by the market share that overseas industries could potentially capture and took a very short-medium term view. The tables were turned when cheap and cheerful vehicles revealed their true colours – rust, unreliability and poor build quality. However, the opposition quickly regrouped and learned the lesson of quality control, customer service and efficiency. Within a few generations the hegemony of the US and European motor manufacturing industry was shattered. 2011 figures have the US 4th, with China, Japan and Germany taking 1st to 3rd place. The same process is taking place in the technology sector, and labour costs notwithstanding, we need to re-examine our relationship with the consumer.

Money is an artifact with a particular form of insidious alchemy. Before it leaves the customers hands, the amount of attention, psychology and manipulation in the form of advertising and promise that is exerted is quite staggering. Once the deal is done and the exchange is made, the level of commitment to the customer frequently falls off a cliff and they are then pointed towards the cold hard small print or the Service Level Agreement. All the promises, the wooing, the roses and chocolates are ultimately revealed for what they are – a cheap play to get inside the wallet. This is what galls me most about exceptions management in that it so neatly encapsulates the whole breakdown in the relationship – after all it was only a one night stand or maybe an affair.

No, unlike this horrific transformation from a flexible analogue relationship to a harshly binary digital one, customer service needs to resolutely, staunchly stick to an idealistic principle. That principle will depend very much on the brand, but to summarise it is "know your customer". Not just in terms of metrics, what they want to buy, their aspirations or ideals. To understand your customer you need to be a servant, after all they have placed their dreams in your hands as the tokens or beads they have given your organisation in the form of money you will never be able to accurately value . Was it paid on a credit card or saved for over years? Earned by the sweat of their brow or theft? Corporatism leaves no room for moral values, as money is one of the most reagent chemicals in the ethical periodic table. It democratises, devalues and frequently dehumanises. To truly serve the customer, you need see beyond this, and ultimately customer service is one of the most ethically challenging roles within an organisation, balancing internal and external ethics. Go that extra mile, spend that time outside your allotted 30 minutes to close that call. A servant is never greater than their master, and while the word "service" is still in the job title, that is in reality what you are to the customer.

**ABOUT THE AUTHOR**

*Rob Somerville has been passionate about technology since his early teens. A keen advocate of open systems since the mid-eighties, he has worked in many corporate sectors including finance, automotive, airlines, government and media in a variety of roles from technical support, system administrator, developer, systems integrator and IT manager. He has moved on from CP/M and nixie tubes but keeps a soldering iron handy just in case.*

# Augmented Reality Law, Privacy, and Ethics

## Law, Society, and Emerging AR Technologies

**BRIAN D. WASSOM, ALLISON BISHOP, TECHNICAL EDITOR**

To the two mentors who had the most meaningful influence on the first 15 years of my professional career. The Honorable Alice M. Batchelder personifies integrity and excellence, and taught me to respect the legal system. Herschel P. Fink, Esq. taught me to love the law I practice, and to practice the law I love. Both gave me amazing opportunities to serve in ways that fundamentally shaped my career. I hope to pay forward to others all that I can never repay to them.

Intellectual property laws protect ideas, creative expression, commercial goodwill, and other intangible concepts. Although they cannot be seen or touched, these concepts have become some of the most valuable assets in our contemporary, knowledge-driven economy. They will remain just as important, if not more so, in a world with ubiquitous augmented reality.

## PATENTS

### THE NATURE OF PATENT PROTECTION

A patent conveys a property right to the inventor(s) of an invention. In the language of the statute and of the patent registration itself, the right granted by a U.S. patent is "the right to exclude others from making, using, offering for sale, or selling" the invention in the United States or "importing" the invention into the United States. To get a U.S. patent, an application must be filed in the U.S. Patent and Trademark Office (USPTO). Patent protection lasts for up to 20 years from the date of application, subject to the payment of appropriate maintenance fees for a utility patent.

Utility patents are the type of patents most relevant to AR. These may be granted to anyone who invents or discovers any new and useful process, machine, article of manufacture, or compositions of matters, or any new useful improvement thereof. In order to receive protection, the inventor must describe the method by which his or her invention would work. Until 1880, the USPTO required that inventors submit working models of their inventions.[1] Since that time, however, an applicant need only describe their concept in the patent application in order to receive protection; they need not actually create something in order to have invented it.

United States law also no longer entitles the one who first invents something to the patent protection on it.

It used to be that even if someone else beat you to the punch in applying to register an invention, you could undo their patent by proving that you invented it first. No longer, thanks to the America Invents Act that President Obama signed into law on September 16, 2011. As of 2013, it is now the "first to file," not the "first to invent," who wins. That is the system that Europe and virtually the entire rest of the world already used.
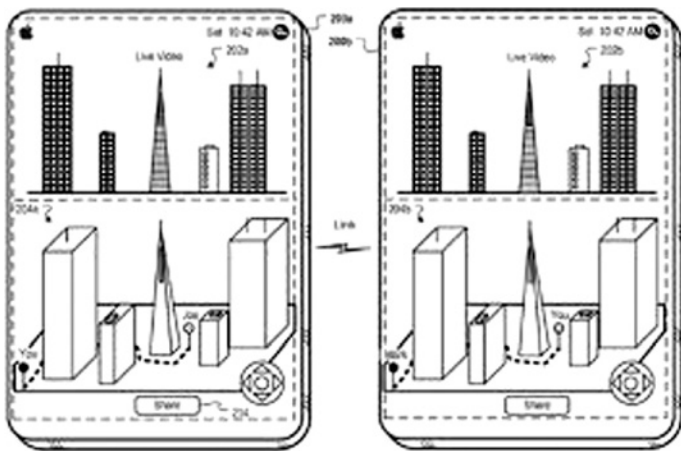


Figure 1. *Apple's 2011 patent application showing AR on an iPad*

## PATENT PROTECTION IN AR INVENTIONS

Tangible, consumer-level AR applications have only recently begun to emerge because we have only recently devised the hardware and software required to make them commercially feasible. Many of these developments, however, have been anticipated for quite some time, which means that many creative minds have already had plenty of time in which to obtain patents on AR-related inventions.

On July 7, 2011, the USPTO published Apple's patent application US 2011/0164163 A1, for "Synchronized, Interactive Augmented Reality Displays for Multifunction Devices (Figure 1)." [2] This news, and the accompanying drawings depicting AR at work on an iPad, caused quite a stir in the blogosphere and among AR enthusiasts, who took it as an indication that the era of mass-market AR was finally about to begin.

But AR has been in the process of "emerging" for years now – plenty long enough for all sorts of companies and inventors to get their ideas registered with the USPTO. These registered inventions include augmented tattoos, advertising on flying footballs, and adding virtual displays to live sporting events (Figure 2).

There is, of course, still plenty of room for innovation in the augmented reality field – just not quite as much room as some might assume. As of Dec. 10, 2011, a search for



Figure 2. *Additional excerpts from AR-related patents*

"augmented reality" in the Google Patents search engine returned about 11,100 hits. In January 2014, that number was up to 160,000.

Moreover, as anyone reading the tech headlines in the past decade realizes, patent litigation is all the rage nowadays. Anyone and everyone with a patent, it seems, is suing or being sued by a competitor with a similar patent or product. In 2012, over 5,000 patent infringement lawsuits were reportedly filed – a spike of over 30% from the year before – and this trend "shows no signs of cooling off, either as a means of generating revenue or of protecting competitive advantage." [3]

This is especially true with respect to smartphones and tablets[4] – precisely the platforms on which consumer AR is just starting to take off. Therefore, we can expect patent litigation to be one of the first areas in which AR-related legal disputes arise in earnest.

## THE FIRST AR PATENT INFRINGEMENT CASE: TOMITA V. NINTENDO[5]

As ominous as the trends of patent litigation can appear from a macro level, the facts of any particular case often seem entirely ordinary, even mundane. That was the case with the earliest recorded litigation activity related to AR.

On June 26, 2012, a judge of the U.S. District Court for the Southern District of New York issued what appears to be the first substantive decision in an AR-related patent infringement case. The device in question was one of the most popular AR-capable units then on the market: the Nintendo 3DS portable game console. Although the

2    U.S. Patent No. 8,400,548 (filed January 5, 2010) available at https://docs.google.com/viewer?url=patentimages. storage.googleapis.com/pdfs/US8400548.pdf.

3    Chris Barry, et al., 2013 Patent Litigation Study: Big Cases Make Headlines, While Patent Cases Proliferate, available at http://www.pwc.com/en_US/us/forensic-services/publications/ assets/2013-patent-litigation-study.pdf.
4    See Topics, Patent Lawsuit, Mashable, http://mashable.com/category/patent-lawsuit/ (last visited June 10, 2014) for articles discussing articles discussing patent disputes between major phone and tablet makers.
5    Tomita Techs. USA, LLC v. Nintendo Co., Ltd., No. 11-Civ-4256 (JSR), 2012 WL 2524770,(S.D.N.Y. 2012)

case had been first filed in June 2011, this was the first substantive decision from the court on the merits of the case, and the first to mention AR.

Plaintiffs ("Tomita") were the owners of U.S. Patent No. 7,417,664, issued in August 2008 and titled "Stereoscopic image picking up and display system based upon optical axes cross-point information." As described by the court, "the '664 patent attempts' to provide a stereoscopic video image pick-up and display system which is capable of providing the stereoscopic video image having natural stereopsis even if the video image producing and playback conditions are different."[6]

Tomita alleged that the 3DS infringes this patent. The June 26, 2012 opinion rejected Nintendo's motion to dismiss the case. The court determined instead that there was enough evidence to allow the case to proceed to a jury.

Most of the discussion in the parties' arguments and the court's opinion focuses on how the 3DS's cameras work to capture 3D images. The patent describes a "means for measuring cross-point (CP) information on the CP of optical axes of [the] pickup means." The two cameras built into the 3DS are arranged in parallel, but the parties and their experts disagreed over whether the optical axes of these cameras would nevertheless intersect. The court agreed with Tomita that they would.

In addition, as described by the court and the parties, the system described by '664 patent includes a "manual entry unit" through which the viewer can change "the operation condition of the display control circuit." The 3DS has at least two modes: "Camera" mode and "AR games" mode. And it has two means of adjusting the threedimensional image it displays: a circle pad and a "3D depth slider." In both the camera application and the AR games application, the 3DS's 3D depth slider only changes the display from a two-dimensional image (turning the three-dimensional display "off") to a three-dimensional one (turning the three-dimensional display "on"). The dispute over this feature was whether, by turning three-dimensional viewing on or off, the 3D depth slider operates as a "manual entry unit" within the offset presetting means' structure. To infringe the '664 patent, "the relevant structure" in the 3DS must "perform the identical function recited in the claim."[7]

The court found that "a reasonable jury could find that the 3DS's 3D depth slider constitutes a component of the offset presetting means' structure," performing one aspect of the identical function recited in the claim. "Specifically," it continued, the '664 patent notes that the "manual entry unit may be [a] switch.. . which is actuated by the viewer depending upon user's preferences for chang-

ing the operation conditions of the display control circuit." Both parties acknowledge that the 3D depth slider functions in the AR Games application as a "switch," allowing the user to exercise control over the display control circuit's operation conditions. Specifically, the 3D depth slider allows the viewer to determine whether the display circuit presents an offset at all. Thus, a reasonable jury could find that the manual entry unit, along with the circuits described in the '664 patent, performs the function of "offsetting and displaying" video images by allowing the user to determine whether the circuits will display an offset.[8]

On this basis, the court allowed Tomita to pursue its claim that, because the unit's 3D depth adjustment switch allows users to adjust the 3D image they see while in "AR Games" mode, the 3DS allegedly infringes the '664 patent.

On March 13, 2013, the jury returned a verdict in Tomita's favor, and awarded it $30.2 million in damages although the judge in the case had decided as a matter of law that Nintendo had not infringed the patent willfully. Both sides filed motions seeking to adjust these rulings. Nintendo prevailed on one important argument – the amount of the damages award, which was based on the estimated value of a reasonable royalty payment by Nintendo to Tomita for use of the technology. The jury had apparently based its figures on the testimony of Tomita's expert, who used the "entire market value" of the 3DS as the royalty base for calculating the reasonable royalty rate. This led the jury to a rate of just under 3% of the 3DS's sale price.

In an August 14, 2013 opinion, the judge found this rate "intrinsically excessive," for a number of reasons. For one thing, the 3DS itself was not profitable. Nintendo makes its money on the sale of 3DS games, but the evidence showed that "the vast majority of games designed for the 3DS do not require or even utilize the technology covered by the '664 patent." It also struck the judge as unfair to consider the entire value of the 3DS game market when "the '664 patent's technology was used only in two features – the 3D camera and the AR games application – and thus was in some sense ancillary to the core functionality of the 3DS as a gaming system."[9] In other words, the court found as a matter of law that any AR functionality in the 3DS is an add-on, rather than a core feature, of the console.

As a result, the judge gave Tomita two choices – either accept a 50% cut in the jury's award, reducing it to $15.1 million, or else conduct a whole new trial on damages. The legal term of art for this ruling is "remittur."

I have reproduced the details of this litigation to demonstrate what patent infringement litigation looks like.

6    Id. at *1.
7    d. at *3
8    8Id. at *7.
9    Tomita Technologies USA, LLC v. Nintendo Co., Ltd., No. 11-cv-4256 (JSR), 2013 WL 4101251, at *10 (S.D.N.Y. August 14, 2013)

Obviously, it hinges on the tiniest of details in the subject inventions and challenged products. Moreover, the ultimate decisions will be rendered by a judge or jury who is unlikely to be knowledgeable in the art, so much depends on how well the issues are explained to them. And in the end, the amount of money at stake in even the most inconsequential AR patents may be significant.

## PATENTS AS WEAPONS OF COMPETITION: 1-800-CONTACTS V. DITTO TECHNOLOGIES

Ditto Technologies launched in 2012 as an innovative leader in "virtual try-on" technology for eyewear. It employed webcam-based AR to show consumers what a particular pair of glasses would look like on them. This apparently caught the attention of its more-established competitor, 1-800-Contacts. According to the Electronic Frontier Foundation, which came to Ditto's defense, "1-800-Contacts' CEO went onto Ditto's website the very day it launched, presumably to investigate the upstart competitor's new technology. Having seen Ditto's product, 1-800-Contacts then went out and purchased a patent from a defunct company that claims to cover selling eyeglasses over a network using a 3D model of a user's face."[10] At the time the lawsuit was filed, 1-800-Contacts still did not offer a competing service, but said that it intended to launch one soon on its Glasses.com site. That app was eventually released for iOS and Android in January and February of 2014, respectively.

What angered the EFF even more was what it perceived to be the strategy behind the lawsuit. Rather than seeking a royalty from Ditto, said the EFF, 1-800-Contacts "seems determined to put Ditto out of business. Period."[11] 1-800-Contacts disputes EFF's characterizations, and claims it has tried to settle the case.[12] The parties actively litigated the case for several months, but in November 2013 it was stayed pending the result of Ditto's request that the U.S. Patent Office re-examine the patent's legitimacy – a long-shot procedural tactic available to defendants in these situations.

The attention given to this dispute contributed to the already active conversation about whether litigation like this and the patents underlying them threaten to squelch innovation in software development. No one entity has done more to raise alarm bells on that issue within the AR community, however, than Lennon Image Technologies, LLC.

## THE FIRST AR PATENT TROLL: LENNON IMAGE TECHNOLOGIES

Lennon is what the patent world calls a "non-practicing entity," or NPE – more commonly referred to as a "patent troll." Such companies own patent rights, but do not use them to make or do anything; rather, their only business is to sue other companies for (allegedly) infringing the patents. The patent troll phenomenon is one of the primary drivers behind the explosion in patent infringement litigation; one report found NPEs responsible for more than
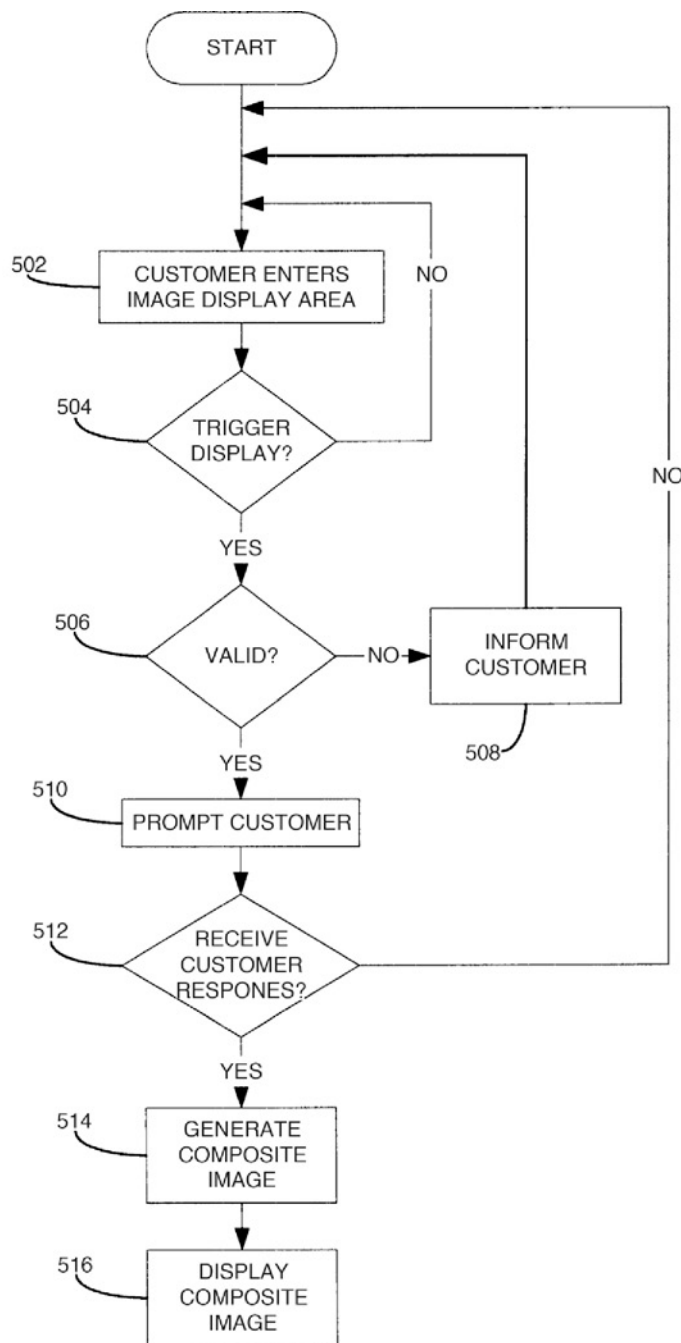


**Figure 3.** *An image from Lennon's patent*

10  Daniel Nazer & Julie Samuels, UPDATED: Help Stop 1-800-Contacts from Abusing Patents to Squelch Competition, Electronic Frontier Foundation (April 17, 2013) https://www.eff.org/ deeplinks/2013/04/1-800-contacts-buys-patent-squelch-competition.
11  Id.
12  Anthony Ho, "Ditto Defeats Patent Claim After Teaming Up With A 'Troll,'" TechCrunch, October 12, 2013, available at http://techcrunch.com/2013/10/12/ditto-wins-defeats-patent-claim-after-team- ing-up-with-a-troll/

half of the patent lawsuits file in 2012, compared to less than a quarter in 2007.[13] Yet only 16% of the cases actually decided by a court were filed by NPEs, "reveal[ing] a much higher tendency for NPE actions to be resolved without a formal court decision."[14] This corresponds to the anecdotal experience that most companies have with patent trolls; they leverage the threat of infringement liability and the steep expense of patent litigation to coerce an early, favorable settlement out of those they sue.

On July 16, 2012, Lennon filed six separate patent infringement lawsuits, all in the U.S. District Court for Delaware. Each is nearly identical to the other, and is based on the same patent: US 6,624,843 B2, issued Sep. 23, 2003.[15] The title of the patent is "Customer Image Capture and Use Thereof in a Retailing System." The abstract describes an AR "virtual try-on" experience very similar to what we see on websites from Ditto and several other retailers (Figure 3):

*In a retailing system, an image capture system is provided and used to capture reference images of models wearing apparel items. At a retailer's place of business, an image capture system substantially identical to that used to capture the reference images is also provided. A customer has his or her image captured by the image capture system at the retailer's place of business. Subsequently, when the customer is in close proximity to an image display area within the retailer's place of business, a composite image comprising the customer's captured image and one of the reference images may be provided. The composite image may comprise full motion video or still images. In this manner, the customer is given the opportunity to virtually assess the selected merchandise without actually having to try on the apparel.*[16]

Of course, one important difference between this abstract and what these defendants do is that current virtual fitting experiences happen online, rather than "within the retailer's place of business." One wonders if that will make a difference in the litigation.

Each of Lennon's complaints specifies a specific website using analogous virtualfitting technology. Among these is Mattel's BarbieDreamCloset.com, which an AR company named Zugara designed and launched. This was the only complained-of site that remained active in the days immediately following Lennon's suits, perhaps because Zugara had recently obtained its own patent[17] for similar technology. Lennon's other lawsuits targeted jewellery-

fitting sites run by Boucheron, Forevermark, De Beers, and Tatler Magazine; a watch-fitting site run by Swatch's Tissot brand; and Skullcandy's headphone-fitting site. On each of these sites, the "virtual try-on" features were removed shortly after the companies behind them were sued (Figure 4).
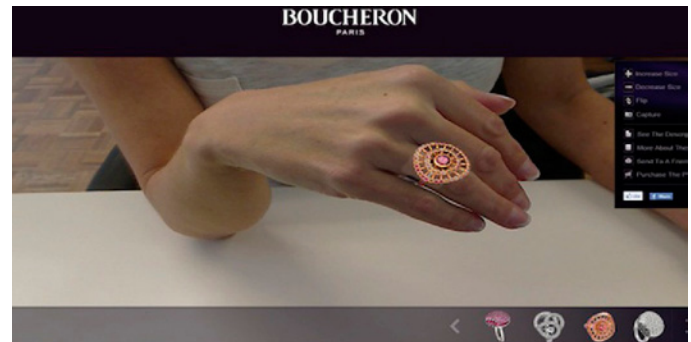


**Figure 4.** *The Boucheron virtual try-on site shut down by Lennon Image Technologies' lawsuit*

This illustrates another tactic commonly employed by patent trolls – suing the end user of the technology, rather than the software company that designed the website.[18] In each of these cases, the AR technology behind the virtual try-on component of the website was supplied by a relatively small software company, yet only the big-name brands publicly using the sites were named. The reason is simple: economics. Not only are these brands more likely to be able to afford to pay a monetary settlement, but they also have far less motivation to fight back against the lawsuit. To them, after all, these AR features were merely interesting but one-off promotional experiments. Losing them prematurely was inconvenient, but hardly significant to the retailers' overall bottom line. It made much more economic sense to pay an early settlement than to invest in defending costly litigation over another company's technology.

The AR companies, however, rely on the software they sell for their very existence, and are generally more likely to be start-ups without the liquid funding necessary to defend such litigation. Some of them may have settled, but if they could afford to fight, they would have been much more likely to resist the litigation to the bitter end and potentially defeat Lennon's asserted patent rights. None of that would have made economic sense for Lennon. So instead, Lennon delivered these companies a double whammy – not only did the lawsuits put an end to the AR companies' existing customer relationships, but they also likely scared away many potential clients who would not risk patent litigation.

---

13   Chris Barry, et al., Patent Litigation Study, supra note 3, at 3.
14   Id. at 3
15   U.S. Patent No. 6,624,843 (filed December 8, 2000).
16   Id. at 1
17   See U.S. Patent No. 8,711,175 (filed August 12, 2011) bool.html&r=1&f=G&l=50&co1=AND&d=PTXT&s1=8,275,590&OS=8,275,590&RS=8,275,590
18   See Dennis Crouch, Patent Trolls by the Numbers, PatentlyO Patent Blog (March 14, 2013) http://patentlyo.com/patent/2013/03/chien-patent-trolls.html

And, of course, once the first round of defendants pay their settlement money, this gives the trolls cash on hand to fund another round of lawsuits. That is exactly what Lennon did in March 2013, filing six more identical lawsuits, this time in the U.S. District Court for the Eastern District of Texas. These lawsuits name Macys Inc., Bloomingdales, Fraimz LLC, Lumondi Inc., Luxottica Retail North America Inc., Safilo America Inc., and Tacori Enterprises. Again, the allegations revolve around "virtual try-on" and "magic dressing room" technology used by these retailers to give customers at home a chance to see on their computers in three dimensions what a product would look like on them. Just as happened after the prior round of lawsuits, the defendants appear to have deactivated the features on their websites as a precaution. Whether they launch again will likely depend on how the lawsuits resolve.

This sort of litigation activity is worrisome for the nascent augmented reality industry, which is still made almost exclusively of small, ambitious start-ups. "Magic mirror" and "virtual dressing room" technology has been a staple of early AR innovations, and (as these lawsuits demonstrate) has really begun to catch on with retailers and customers alike. On the other hand, developments like this were easy to anticipate. As AR starts to attract real money, we can expect it to give rise to at least as many patent fights as the mobile phone industry is currently dealing with.

Ditto became a poster child for this phenomenon. In a tragic twist of fate, in addition to its dispute with 1-800-Contacts, Ditto was also one of the companies sued by Lennon. This was one of the lawsuits studied in a subsequent study by Catherine Tucker, a professor of marketing at MIT's Sloan School of Business that attempted to quantify the economic impact of patent troll litigation on the economy. According to Tucker's study, even though Ditto eventually resolved Lennon's lawsuit, "the company was still being valued at $3 to $4 million less than it would be otherwise, and it was forced to lay off four of its 15 employees to pay legal expenses."[19] In total, Tucker estimated that lawsuits, the most active patent trolls, cost the U.S. economy more than $21 billion. Let us hope that litigation like this does not unnecessarily deter developers from pushing AR technology forward.[20]

## TRADEMARKS

Although AR-related patent infringement has already begun, it is in the area of trademark law where I expect AR to begin breaking new ground in intellectual property law. Hundreds of innovators have already anticipated and sought patent protection for AR inventions, but the technology is only now entering into the consciousness of consumer-level retailers and marketing professionals.

## TRADEMARK BASICS

A trademark is "a word, phrase, symbol, and/or design that identifies and distinguishes the source of the goods of one party from those of others."[21] Technically, a mark that distinguishes services rather than goods is called a "service mark," although the term "trademark" is often used to refer to both,[22] as it will be here. A mark need not explicitly identify the source of the goods or services – it may be suggestive, as many logos are – but the mark must be distinct enough to indicate one source and no other. In this way, trademarks perform an important role in our consumer-driven society, by providing consumers an efficient means to locate products from the providers they trust, and by allowing businesses to protect the integrity of, and goodwill in, their commercial identities.

A person or entity infringes upon the trademark rights of another by interfering with the trademark's ability to signify the goods or services of its owner. This can happen by adopting a mark that is so similar to a pre-existing mark that consumers are confused as to which mark signifies which source, or by using someone else's trademark in an unapproved manner. Courts assess whether trademark infringement has occurred by measuring the "likelihood of confusion" presented by the facts of a particular case. The particulars of this test vary from court to court, but they always involve some variation of the following:

1. The similarity or dissimilarity of the marks in their entireties as to appearance, sound, connotation, and commercial impression.
2. The similarity or dissimilarity and nature of the goods. .. described in an application or registration or in connection with which a prior mark is in use.
3. The similarity or dissimilarity of established, likely-to-continue trade channels.
4. The conditions under which and buyers to whom sales are made, i.e. "impulse" vs. careful, sophisticated purchasing.
5. The fame of the prior mark.
6. The number and nature of similar marks in use on similar goods.
7. The nature and extent of any actual confusion.

19  Joe Mullin, "New study suggests patent trolls really are killing startups," Ars Technica, June 11, 2014, available at http://arstechnica.com/tech-policy/2014/06/new-study-suggests-patent-trolls-really- are-killing-startups/
20  On September 15, 2012, a request was filed with the U.S Patent & Trademark office to re-examine Lennon's patent. As of this writing, that request had not yet been acted on. Meanwhile, several of the cases in Delaware and Texas remained ongoing.

21  United State Patent and Trademark Office, Trademark, Patent, or Copyright, USPTO.gov (January 18, 2013) http://www.uspto.gov/trademarks/basics/definitions.jsp.
22  See Id.

8.  The length of time during and the conditions under which there has been concurrent use without evidence of actual confusion.
9.  The variety of goods on which a mark is or is not used.
10. The market interface between the applicant and the owner of a prior mark.
11. The extent to which applicant has a right to exclude others from use of its mark on its goods.
12. The extent of potential confusion.
13. Any other established fact probative of the effect of use.[23]

Not all of these factors may be relevant or of equal weight in a given case, and any one of the factors may control a particular case.



**Figure 5.** *The user-modulated AR ads in Keiichi Matsuda's video short, Domestic Robocop*

One obtains trademark rights by using the mark in commerce, but registering the mark with the U.S. Patent and Trademark Office gives the owner an even broader range of protection. Trademarks are governed on the Federal level by the Lanham Trademark Act of 1946, as amended,[24] as well as a variety of state laws. In a conflict between two trademarks, the one that began to be used (or was registered) first has priority over the other.

Not all trademarks receive the same degree of protection by the courts. In general, the more distinctive the mark is, the more protection it is afforded. In some cases, even a mark which is not by itself distinctive can still be protected because it has acquired "secondary meaning" in the market – in other words, a mark that is indistinct in the abstract can come to be generally understood as signifying a particular source. Courts place marks on a sliding scale of distinctiveness, generally dividing that spectrum into the following five categories:

- Fanciful: These receive the highest protection available under the Lanham Act. They have no logical meaning or alternative meaning and were invented solely to identify goods. Examples include KODAK and XEROX.
- Arbitrary: Slightly less protected than fanciful marks, but still considered a strong mark. These marks have no logical relation to the goods they are identifying. Examples include APPLE (as applied to computers), BLACKBERRY (for phones), and LOTUS (for software).
- Suggestive: Weaker than arbitrary marks, but still inherently distinctive. These marks evoke a characteristic of the good it identifies, but the viewer must make a mental inference to connect the mark to the product. Examples include CHICKEN OF THE SEA (for tuna), GREYHOUND (for buses), and COPPERTONE (for suntan lotion).
- Descriptive: Weaker than suggestive marks because they merely describe a characteristic of the product or service with no mental inference required. They are not protected as trademarks unless they have acquired a "secondary meaning" over time. Examples include SUDSY SOAP, ALL BRAN and VISION CENTER.
- Generic: These marks can never be protected as trademarks and are free to be used by anyone because they are basic, common descriptors for the category into which the product or service fits – such as "tape,' "shirts," or "computers." Some marks that were once distinctive can become generic – and therefore unprotectable – by becoming publicly used as a generic term. Examples of words that were once trademarks but became generic include ASPIRIN and CELLOPHANE.

We can be certain that, as digital content gets published in augmented media, trademark-laden commercial content will follow. Perhaps the most extreme (and disturbingly plausible) depiction of "sponsored" augmented reality can be found in Keiichi Matsuda's short video *Augmented (hyper)Reality: Domestic Robocop.*[25] The AR user in this video sees literally every flat surface in his modest kitchenette digitally plastered with branded advertisements. At one point he even manually raises the "advertising level" of his eyewear, suggesting that he's receiving micropayments or subsidized services for each ad he sees (Figure 5).

With that consumer-facing communication come inevitable questions of how commercial goodwill is being used to attract consumer attention. That is the realm of trademark law. Because AR will enable various

23  See, e.g., In re E.I. du Pont de Nemours & Co., 476 F.2d 1357 (C.C.P.A. 1973).
24  15 U.S.C. §§ 1051–1141n.

25  Keiichi Matsuda, Augmented (hyper) Reality: Domestic Robocop, Youtube (January 6, 2010) http://www.youtube.com/watch?v=fSfKlCmYcLc

forms of communication that have not previously been seen, many of the related trademark questions will also be novel.

## EXPANDING TRADEMARK LAW BY AUGMENTING NEW SENSES

Anything that distinguishes the source of a good or service can be a trademark. Although trademarks are often thought of as words or graphical designs, the term is also defined to include "symbols," which can encompass almost anything. Such exotic marks as such as scents, sounds, and colors have been registered in the past. Examples include the lion's roar at the beginning of MGM films, the sound a Harley Davidson motorcycle makes when it starts, and the tones at the end of an Intel commercial.

Emerging AR technologies have already inspired a wide variety of conventional trademarks, including words, logos, and phrases. Soon, though, technologies that augment our sense of touch may lead to a rush of trademark applications seeking to protect a wide variety of artificial textures. As discussed in Chapter 2, a number of companies from Senseg to Disney to Apple are experimenting with different means of tricking the mind into thinking one's skin is perceiving whatever haptic sensation a content provider wishes to convey. The potential of AR will never be fully realized until users can reach out and touch virtual objects through haptic interfaces. One way this technology seems likely to (literally) get into the hands of consumers is through retailers using haptic technology to further enhance the "feel" of their products. When that begins to happen, I believe we will witness a resurgence of interest in haptic trademarks. (Other trademark practitioners have called these "tactile," "texture," or even "touch" marks, but I prefer the more definitionally sound and technologically consistent term "haptic.")

Of the less-conventional trademarks, haptic marks are among the least common. Those commentators who have broached the subject in recent years[26] have only identified a handful of such federally registered marks. They include a registration by American Wholesale Wine & Spirits for "a velvet textured covering on the surface of a bottle of wine"[27] –specifically, its Khvanchkara brand of wine. In the course of convincing the U.S. Patent and Trademark Office to register this mark, American Wholesale distinguished its "velvety covering" from that of the more iconic Crown Royal bag by noting that Khvanchkara is "tightly encased within the fabric," and that the "FEEL of a LIMP

bag is quite different from the FEEL of a TURGID velvety surface attached to a wine bottle."[28] Similarly, Touchdown Marketing has registered a trademark in the "pebble-grain texture" and "soft-touch feel" of its basketball-shaped cologne dispenser, and Fresh, Inc. has registered the "cotton-textured paper" that wraps its soap products.

Conceptually, a distinctive touch ought to be just as protectable by trademark law as any other unique indicator of source. Indeed, in 2006, the International Trademark Association (INTA) adopted "a resolution supporting the recognition and registration of 'touch' marks."[29] In practice, however, it is very difficult to separate the way something feels with the function that texture performs – and to come up with a texture that is truly "distinctive" of one product as opposed to other brands within the same category of products.

That is where haptic AR technologies like the ones proposed by Senseg and other companies come in. The ability to coat the surface of any product with a transparent layer of "tixels" capable of mimicking any arbitrary texture the manufacturer chooses would finally break the connection between a product's feel and the function it performs. Consider, for example, a book cover that feels wet, or a plastic squirt gun that feels metallic. There is no necessary correlation between what these products are or what they do, and the way they feel. There should, therefore, be no conceptual barrier to those manufacturers seeking trademark protection in those textures.

Of course, not every artificial texture will automatically be eligible for trademark protection. Many haptic enhancements may still be chosen for functional reasons. The maker of an automotive steering wheel or a baseball, for example, might choose to make their products artificially sticky to enhance performance. A cell phone might be designed to get warmer in one's pocket as it rings, in order to catch the user's attention.[30] And it could be that certain haptic enhancements still do not rise to the level of being sufficiently distinctive of a particular source to serve as a trademark. Still, by promising the ability to manipulate the sensation of touch independently from other aspects of a product, haptic AR technologies open up a new and exciting world of trademark possibilities. Consumers may soon reach out and touch … whatever retailers want them to.

## KEYWORD ADVERTISING IN THE AUGMENTED MEDIUM

The growth of the commercial internet over the past 20 years has been funded predominately by advertising revenue.

26  See Steve Baird, Touch Trademarks and Tactile Brands With Mojo: Feeling the Strength of a Velvet, Turgid, Touch Mark?, Duets Blog (July 13, 2009) http://www.duetsblog.com/2009/07/articles/trademarks/touch-trademarks-and-tactile-brands-with-mojo-feeling-the-strength-of-a-velvet-turgid-touchmark/
27  U.S. Trademark Application Serial No. 76,634,174 (Filed March 23, 2005) available at http:// tsdr.uspto.gov/-caseNumber=76634174&caseType=SERIAL_NO&s.

28  Response to Office Action, U.S. Trademark Application Serial No. 76,634,174 (April 17, 2006) available at http://tsdr.uspto.gov/documentviewer?caseId=sn76634174&docId=ROA20060418121514#docIndex=4&page=1
29  Report of the World Intellectual Property Organization, Standing Committee On The Law Of Trademarks, Industrial Designs And Geographical Indications, Sixteenth Session, Geneva, November 13 to 17, 2006 at 10-11 (2006).
30  Technically, as noted in Chapter 2, the ability to discern heat is distinct from the sense of touch. For simplicity's sake, however, this book will follow the popular approach of treating them as the same.

We as consumers get to browse free content on millions of web pages and on various search engines in large part because advertisers have paid good money to insert their ad next to whatever we're reading. Odds are good that this funding model will continue well into the future.

The primary purpose of all commercial advertising is to draw potential customers to the advertised business or product, and away from its competitors. Moreover, as mentioned in Chapter 4, comparative advertisements – those that compare a product to its competition – have been around for decades. Courts have had opportunities to draw some basic lines between what is okay to say in such advertisements, and what is "deceptive" advertising. In a nutshell, it is permissible to describe your competitor's goods and compare one product to another, but you cannot say things that are likely to confuse customers into believing that you *are* your competitor. You cannot say something materially false or misleading about your competitor or your own product. And you cannot do anything to confuse reasonable consumers into mistakenly believing there's some sort of connection, sponsorship, affiliation, or endorsement between your companies or products.

These boundaries are not always easy to apply, however, and there are several contexts in which the courts have not been able to agree on how they apply. For example, the battle over "keyword advertising"–i.e., using an algorithm to display a "sponsored" ad whenever a user types a given term into a search engine–is still being fought, more than a decade after the practice began.

Google explained its own keyword advertising system, called "AdWords," this way:

Google AdWords is Google's advertising program. AdWords lets you create simple, effective ads and display them to people already searching online for information related to your business. So how is it possible to show your ads only to the most relevant audiences? The answer is keyword-based advertising.

*When a searcher visits Google and enters a query – say,* good beginner guitars – *Google displays a variety of relevant search results, such as links to articles containing guitar purchasing advice, or websites dedicated to novice musicians. Google also displays AdWords ads that link to online businesses selling guitars, music lessons, or other products and services related to the query.*

*For example, imagine that you own a music store carrying a large selection of guitars. You could sign up for an AdWords account and create ads for entry-level guitars in your inventory. For each of your ads, you might select keywords (single words or phrases related to your ad's message) such as* beginner guitars *or* entrylevel guitars.[31]

Company A potentially implicates trademark law when it purchases a search term that is also a trademark belonging to Company B. The fact that Company A's advertising appears when a user searches for Company B's trademark raises questions of whether Company A is "using" that trademark "in commerce" (most courts have said yes), and whether this use creates a likelihood that consumers will be confused regarding the potential association or sponsorship between the two companies or as to the source of Company B's goods or services. Answers to this latter question have been mixed. Some courts over the past decade have found that ads triggered by a trademarked keyword search cause a likelihood of confusion – especially when the resulting ad also incorporates the trademarked term,[32] but even occasionally when it does not.[33] On the other hand, several recent cases have rejected the proposition that merely purchasing a competitor's trademark as a search term in and of itself creates confusion.[34]

This may suggest that the potential for confusion in many situations has decreased as online sponsored ads have become more commonplace.

Where the potential for confusion exists, though, the question of who is responsible for it also remains open. Rosetta Stone is one of several companies to sue a search engine for allowing competitors to use its marks in keyword ads. As most other courts had done in similar cases, the trial court dismissed the suit as a matter of law, finding that Rosetta Stone could not prove that the search engine was liable. But in April 2012, the U.S. Court of Appeals for the Fourth Circuit overturned that holding, finding it possible that the search engine's policy on the use of keywords in sponsored ads could amount to direct infringement, contributory infringement, or trademark dilution.[35] Other cases have likewise gone either way on liability depending on how the particular trademark at issue appeared in the header or text of a sponsored ad. But it is fascinating that, even as recently as 2013, one study found that more than 40% of search engine users were not able to distinguish sponsored ads from organic search results,[36] suggesting that the potential for confusion remains even more than a decade after this advertising model was adopted.

31  See Google AdWords, http://www.google.com/adwords/learningcenter/text/18911.html (last visited March 23, 2009)

32  See, e.g., Storus Corp. v. Aroa Mktg., Civ. No. 06-2454-MMC; 2008 U.S. Dist. LEXIS 11698, at *12-13 (N.D. Cal. February 15, 2008) (finding infringement where defendant's sponsored ad was triggered by and incorporated plaintiff's trademarked "smart money clip")

33  See, e.g., Edina Realty, Inc. v. Themlsonline.com, Civ. 04-4371JRTFLN; 2006 U.S. Dist. LEXIS 13775 (D. Minn. March 20, 2006) (finding liability where "Defendant purchases search terms that include the Edina Realty mark to generate its sponsored link advertisement"); Fin. Express LLC v. Nowcom Corp., 564 F. Supp. 2d 1160, 1177 (C.D. Cal. 2008) (holding that defendant's purchase of keywords that "are identical or strikingly similar to the trademarks held by plaintiff" along with its offer of "services and products which are highly related to those offered by plaintiff" and "simultaneous use of the Web as a marketing channel" may result in consumer confusion).

34  See, e.g., 1-800-Contacts, Inc. v. Lens.com, Inc., 722 F.3d 1229 (10th Cir. 2013).

35  See Rosetta Stone LTD. v. Google, Inc., 676 F.3d 144 (4th Cir. 2012)

36  Graham Charlton, 40% of Consumers are Unaware that Google Adwords are Adverts, Econsultancy Blog (February 28, 2013) http://econsultancy.com/blog/62249-40-of-consumers-are-unaware- that-google-adwords-are-adverts.

**Figure 6.** *A campaign by the Public Ad Project and the Heavy Projects*



**Figure 7.** *"ADmented Reality" Glass Parody*

Augmented reality will take this jostling for position between advertisers to a new level. We already see this happening in TV broadcasts of certain sports games, in which "digital billboard replacement" technology is used to superimpose digital ads on top of the ones that are physically present in the stadium. The Public Ad Project and the Heavy Projects have demonstrated similar concepts on mobile devices by sponsoring campaigns that replace physical billboards with artistic images when viewed through a mobile device (Figure 6).

But what happens when AR eyewear becomes ubiquitous, and digital ad replacement becomes commonplace? Will advertisers pay AR service providers for the ability to superimpose their ads on top of what consumers see? If the past 20 years of e-commerce is any indication, then the answer is "absolutely"–and in a number of creative ways. So, for example, a business may pay to superimpose its logo on top of signs advertising a competitor's products, completely blocking the physical ad from view. Or, the mere act of looking at Company A's ad through your AR eyewear may trigger a virtual ad for Company B to pop up somewhere else in your field of vision. The example of this that I typically give is of looking at a McDonald's sign through your digital device and instantly seeing a Burger King advertisement superimposed upon it.

Similarly, your decision to look at something may prompt suggestions for goods and services relating to the thing you're looking at. Self-described "pop culture hacker" Jonathan McIntosh captures all of these ideas in his parody video "ADmented Reality."[37] The video depicts a world in which every glance triggers another advertisement in one's digital eyewear, to the point where reality itself become obscured in a sea of sponsored content (Figure 7).
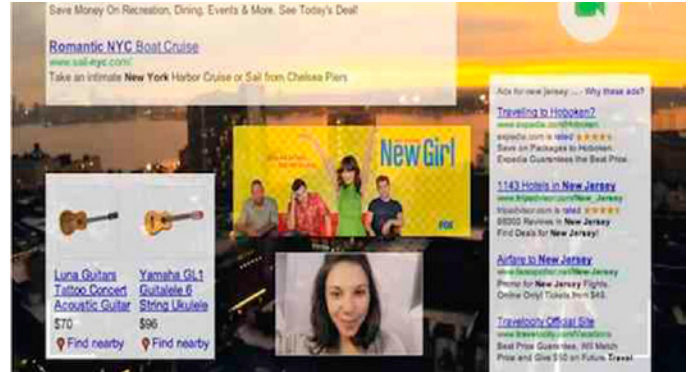
Other commentators have also foreseen augmented advertising and the legal issues they will raise. John C. Havens discussed some of them his insightful piece for Mashable called "*Who Owns the Advertising Space in an Augmented Reality World?*"[38] Noting that Google had already applied for a patent for digitally replacing physical ads within the Street View feature of Google Maps, Havens wrote that "the importance of virtual real estate may quickly supplant actual signage for advertisers. This is especially true when virtual signage could be switched dynamically for individual eye traffic depending on a viewer's preferences."[39] He went on to quote Gabe Greenberg, director of social and emerging media at Microsoft, as saying that, "if the experience presents the ads in a way that makes sense for the augmented reality experience and the user's intention, this could be a powerful advertising tool for tomorrow's marketplace."[40]

These predictions are persuasive. As discussed in Chapter 6, I take issue with the idea of applying the law of real property to this scenario. That is not necessarily the end of the conversation, however, because the laws governing trademarks and unfair competition are not about property ownership. They are aimed at protecting commercial goodwill and avoiding confusion among consumers about the relationships between different products and businesses. Sponsored ads on search engines, for example, do not do anything to obscure the results displayed on a search engine; they are merely displayed adjacent to that content. When Company A displays a sponsored ad next to Company B's trademark, it is not interfering with Company B's ownership of that mark. But – depending on the content of the ad, how it is displayed, and how it comes to appear on the page – Company A might be misleading consumers into believing there is some relationship between Company A and that trademark. This potential for confusion is what injures

---

37 Jonathan McIntosh, Admented Reality, Youtube (April 5, 2012) http://www.youtube.com/watch?v=_mRF0rBXIeg&feature=kp

38 John Havens, Who Owns the Advertising Space in an Augmented Reality World?, Mashable, (June 6, 2011) http://mashable.com/2011/06/06/virtual-air-rights-augmented-reality/
39 40Id.
40 40Id.

Company B and triggers the protections of trademark law.

The potential remains, therefore, that causing Company A's augmented ad to appear in a certain physical place – for example, on top of or next to Company B's physical billboard, place of business, or trademarked logo – may create a likelihood of confusion in the minds of consumers. It will be possible, therefore, for augmented advertising to infringe trademark rights.

At least in the short term, that result seems unlikely, if only because of the limited context in which AR experiences are currently available. Today, having an AR experience requires a user to download and open a particular, branded app on their device. These apps also usually offer only a very limited range of options in a predetermined number of situations. So, for example, as of this writing, the only way a user will see a Burger King ad atop the Golden Arches would be by using an app (or usergenerated layer with an app like Junaio, Aurasma, or Layar) designed specifically for that purpose. In this situation, a trademark owner could object to the way that its trademark is being "used in commerce," and the way in which the app is portrayed could conceivably be confusing. Assuming that the user understands where the app is coming from, however, one can hardly expect the user to be surprised or confused by what they see through it.

The potential for confusion will come within digital services in which consumers expect to see advertising content from a variety of authentic sources within a viewpoint-neutral environment. One does not approach billboards, telephone directories, television commercial breaks, or internet banner ads *as such* with a predetermined expectation of the message those media will contain. Instead, one bases their determination about the source of a particular advertisement within those media based on the content and context of the ad itself.

For example, merely opening my internet browser tells me almost nothing about what sort of banner advertising I might encounter; I know by virtue of having surfed the internet that I will be served such ads by any random company that may have paid to place them there. But if I'm discerning, I will notice that certain types of websites are more likely to serve up advertisements from a particular point of view, and that the behavioral advertising cookies in my browser will sometimes deliver ads based on my prior online activity. Similarly, to the extent that anyone still reads telephone directories, they ought to expect to see advertisements for local businesses (especially personal injury lawyers) rather than for those located elsewhere.

When we have multi-user, viewpoint-neutral augmented reality browsers is when we should expect to see allega-

tions of trademark infringement arise in earnest. The existing ability to digitally replace physical signs within mapping programs such as Bing and Google Maps offers a glimpse of what such a world will be like. Ubiquitous, always-on AR will feel very much like moving around within a three-dimensional version of those contemporary mapping programs. Once we find ourselves there, what expectations will we have about the advertising we see? More than likely, we will realize that at least some of the augmented content we encounter is provided by the service provider itself (whichever company that turns out to be), while some is triggered by our personal activities and preferences. Just as with behavioral advertisements on the internet today, no two users of the service are likely to encounter all of the same ads.

Unlike the current web, however, augmented ads will necessarily correspond to physical places. It will be those relationships between digital and physical content that raise new and unique questions of when a likelihood of confusion may exist. Sticking with the fast food example, then, will it be permissible in *this* context for Burger King to deliver users an ad every time they look in the direction of a McDonald's restaurant or sign? If so, will the law of trademarks and unfair competition place limits on how obtrusive these ads can be? In other words, may they appear only in the periphery of a user's vision? May they hover in space next to the Golden Arches, or even be superimposed over them? Moreover, the degree to which a service provider makes these decisions – or allows users to adjust such settings – could well determine whether the service provider may be held jointly liable for any resulting infringement.

Courts deciding AR advertising cases in these contexts will apply the lessons learned in pre-existing media, including the reasoning of the search engine keyword cases with which today's courts are wrestling. Just as search engine algorithms use particular terms as keywords that prompt an ad to appear, so too can the physical objects that prompt similar virtual ads in AR devices be thought of as "keywords." Whether it's a billboard, logo, or some other trigger, any object that prompts an algorithm to display an ad is performing the same function that keywords do today.

A determination of whether that ad creates a likelihood of confusion will depend on how the likelihood of confusion factors apply to the particular case at hand. As with existing case law on sponsored advertising, moreover, courts are likely to be all over the map in how they decide such cases at first, until the model becomes more commonplace and a consensus forms about what boundaries it is fair to expect advertisers to observe in this space.

## FAIR USE AND FREE SPEECH

Trademark ownership is not a complete monopoly on any and all uses of the word or symbol that forms the trademark. Although trademark rights are broad, they exist only to protect consumers from confusion and to safeguard business's goodwill. As restrictions on the rights of others' speech, moreover, trademark laws always exist in an uneasy tension with the First Amendment to the United States Constitution.

"Because overextension of Lanham Act restrictions in the area of [artistic expression] might intrude on First Amendment values," wrote the Second Circuit Court of Appeals in the frequently quoted opinion *Rogers v. Grimaldi*, "[courts] construe the Act narrowly to avoid such a conflict."[41] That case stands for the proposition that artists can freely refer to trademarked goods and services by name in the titles of their songs, films, and other creative expressions. Such issues will inevitably arise in the context of augmented works just as they do elsewhere. There are at least a couple situations, however, in which augmented content will stretch these legal principles in new ways.

### Incorporating third-party trademarks into augmented content

Trademarks frequently show up inside of artistic works – especially in video games that attempt to create a realistic world in which players can immerse themselves. For the most part, courts uphold these uses as free speech, due in no small part to the United States Supreme Court's decision in 2011 that video games deserve First Amendment protection.[42]

Games and other immersive augmented reality environments will attempt to create similarly realistic digital worlds. In so doing, there will inevitably be some AR applications that recreate actual trademarks in the name of authenticity.

The one fundamental difference between the AR medium and traditional digital expression, however, is that AR content is inherently tied to real physical locations. This distinction adds a layer of risk to replicating someone else's trademark in AR because associating that trademark with a real place or object could, in many foreseeable circumstances, heighten the likelihood that someone will draw a connection between the trademark and the physical place or object with which it is digitally associated. For example, players may see the mark digitally displayed on the wall of a business not associated with the trademark owner, or the mark may appear (wither physically or digitally) on a real object designed to serve as a target within the AR

app. In either circumstance, the mark is no longer confined within a virtual, fictional word created by the artist, but instead is being associated with real objects or places that may be businesses or products with which the trademark owner does not wish to be associated.



**Figure 8.** *Mark Skwarek's "The Leak in Your Home Town" app*

This could, in some cases, satisfy enough of the likelihood of confusion factors to add up to a real headache for both the trademark owner and the designer of the AR environment. Of course, it is equally possible – again, depending on the circumstances of the particular case – that the choice to make that particular association between trademark and physical place or thing could, in and of itself, be a creatively expressive decision that merits First Amendment protection. Regardless of result, however, use of trademarks within AR content will inherently raise an additional dimension of legal complexity beyond that found in other digital works.

### Unauthorized augmentation of trademarks

For the first few years in which AR has been used in advertising, the technology required to create the experience has been more or less limited to corporations, agencies, and startups with substantial budgets, sophisticated software, and coding expertise. Even the first publicly accessible tools for creating user-generated AR contents have been slow to catch on, and required a significant learning curve. As this book nears completion

---

41  Rogers v. Grimaldi, 875 F. 2d 994, 998 (2d Cir. 1989).
42  See Brown v. Entertainment Merchants Ass'n, 1313 S.Ct. 2729 (2011)

during 2014, however, more user-friendly and robust creative tools are hitting the public market, democratizing AR even further. Before long, user-generated commentary is likely to be as ubiquitous in augmented form as video commentary currently is on YouTube.

When the subject matter of user-generated AR content relates to a particular brand, no object will be more tempting to serve as the trigger for that content than the very trademark that the brand owner uses to represent its goodwill to the public. Indeed, this has already happened at least once. In 2010, Professor Mark Skwarek (of the NYU Polytechnic School of Engineering and, most recently, the creative lead behind the Kickstarter-funded app PlayAR) released the iPhone app "The Leak in Your Home Town" (Figure 8). Through this app, one could view a physical sign bearing the BP logo at a local gas station, and see superimposed on that logo a digital broken pipe spewing oil, exactly like the one responsible for the then-current spill in the Gulf of Mexico.

These existing media also teach us that a sizeable portion of that commentary will be directed back toward the brands who advertise to us. For almost as long as companies have been setting up shop at <Company.com>, there have been detractors posting vitriol at <CompanySucks.com>. In today's social media, popular sites such as Ripoff Report and Pissed Consumer base their entire business models on naming and shaming commercial brands.

Although some early judicial decisions blocked these sites' ability to reproduce the trademarks of the companies they criticize, most courts and other trademark dispute resolution organizations recognize such content as fair commentary that trademark holders cannot prevent.[43] For example, in 2011, the United States District Court for the Eastern District of New York rejected a trademark infringement lawsuit that challenged the use of a reviewed company's trademarks in the sub-URLs, metadata, and text of PissedConsumer.com.[44] Despite copious use of the plaintiff's marks throughout the website, the court

found it implausible that any reasonable person would believe the site's critical commentary to be sponsored by or associated with the trademark owner.

These are the types of precedents courts will look to when trademark owners begin to grapple with augmented repurposing of trademarks. They provide a strong basis for predicting that using corporate trademarks as triggers for AR content that criticizes the trademark owner will, in many cases, be permissible under U.S. trademark law. This conclusion is bolstered by considering the similarity between AR targets and hyperlinks, which will be considered in Chapter 6.

Of course, every rule has its exception. The circumstances of each situation will be different, and those differences will sometimes make a material impact on the outcome of a trademark infringement analysis. In cases where the augmented content that one associates with another's trademark is more akin to the competitive advertising discussed above than to critical consumer speech, the question of whether that content causes a likelihood of confusion will be much closer. Nor has this discussion taken into account the concept of trademark dilution, a cause of action that challenges the use of a famous mark in ways that diminish its distinctiveness or tarnish its goodwill, even in ways that do not cause a likelihood of confusion. The application of that doctrine to AR content will also vary widely depending on the circumstances.

What does seem clear, however, is that policing the use of trademarks in augmented reality will be significantly more complex than it first appears.

## COPYRIGHT

AR-related copyright issues may not lead to litigation as quickly as patent and trademark disputes will. In the long run, however, I believe that AR is likely to raise a broader range of copyright matters than any other type of intellectual property issue. After all, the realm of copyright law is creative expression, an activity that (unlike innovation or the creation of commercial goodwill) is potentially available to all. AR is a medium in which all manner of creative ideas will be expressed.

## COPYRIGHT BASICS

United States copyright law is a state-sanctioned, limited monopoly granted to the authors of creative expression. These authors receive the right to control some of the ways in which their works are used. In exchange, ownership of the work reverts to the public domain upon the expiration of the copyright term.

The U.S. Copyright Act specifies eight broad categories of creative "works" to which copyright protection applies:

43  See, e.g., Taubman Co. v. Webfeats, 319 F.3d 770, 777-78 (6th Cir. 2003) (no Lanham Act violation where gripe site with domain name taubmansucks.com that provided editorial on conflict between website creator and plaintiff corporation did not create any possibility of confusion); Taylor Bldg. Corp. of Am. v. Benfield, 507 F.Supp.2d 832, 847 (S.D.Ohio 2007) (gripe site with domain name taylorhomesripoff.com that served as forum for criticizing home builder did not create any likelihood of confusion "because [n]o one seeking Taylor's website would think – even momentarily – that Taylor in fact sponsored a website that included the word 'ripoff' in its website address"); Bally Total Fitness Holding Corp. v. Faber, 29 F.Supp.2d 1161, 1163-64 (C.D.Cal.1998) (gripe site with domain name www. compupix.com/ballysucks dedicated to complaints about Bally's health club did not create likelihood of confusion because no reasonable visitor to gripe site would assume it to come from same source or think it to be affiliated with, connected with, or sponsored by Bally's); MCW, Inc. v. Badbusinessbureau.com, L.L.C., No. 02 Civ. 2727, 2004 WL 833595, at *16 (N.D.Tex. April 14, 2004) (Lanham Act unfair competition claims against consumer review websites called "ripoffreport.com" and "badbusinessbureau. com" that used plaintiff's trademarks in connection with allegedly defamatory posts dismissed because no visitor to websites would believe that plaintiff markholder endorsed the comments on sites); Whitney Inf. Network, Inc. v. Xcentric Ventures, No. 2:04-cv-47-FtM-34SPC, 2005 WL 1677256 (M.D.Fla. July 14, 2005) (unpublished memorandum and order) (dismissing trademark infringement and false designation of origin claims against "ripoffreport.com" because plaintiff mark holder, a seller of education courses, was involved in different field than defendant, who sold advertising space on site and helped aggrieved consumers reclaim lost money, and because no consumer would "be confused by a consumer watch-dog type website that is not selling any real estate investment course"); Cintas Corp. v. Unite Here, 601 F.Supp.2d 571 (S.D.N.Y. 2009), aff 'd 355 Fed.Appx. 508 (2d Cir. 2009) (per curiam) (rejecting assertion by Cintas that the website <cintasexposed.com>, run by a labor union and dedicated to criticizing the company's labor practices, could cause customer confusion).
44  Ascentive, LLC v. Opinion Corp., 842 F. Supp. 2d 450 (E.D.N.Y. 2011)

1. Literary works;
2. Musical works, including any accompanying words;
3. Dramatic works, including any accompanying music;
4. Pantomimes and Choreographic works;
5. Pictorial, Graphic, and Sculptural works;
6. Motion pictures and other audiovisual works;
7. Sound recordings; and
8. Architectural works.[45]

One could easily conceive of how each of these types of works could be expressed by augmented means.

United States copyright law affords to creators five basic rights with respect to their copyrighted work–the rights to control its reproduction, adaptation, distribution, public display, and public performance. These broad categories cover most, but not all of the uses one can make of copyrighted works. The copyright statute also carves out various categories of use over which the copyright owner should not have control. Chief among these is the doctrine of "fair use," which describes a range of activities that benefit society too much to allow copyright owners to squelch them.

## OBTAINING COPYRIGHTS
### Fixation in a tangible medium
Nothing inherent to the AR medium will prevent augmented content from receiving copyright protection. To qualify for copyright protection, the work must be "fixed in a tangible medium," meaning it must have some definite, perceptible form rather than just being evanescent sounds or an inchoate conception floating in someone's head. This requirement provides a measure of objectivity in the application of copyright law, without which society would not be getting anything in exchange for the legal monopoly it grants to a copyright owner. That said, this "fixation" requirement is a loose one. Storing an image in software form is enough; even projecting an image digitally onto a screen or loading software into temporary random-access memory is sufficient.[46] This is what allows digital representations to be copyright-protected in conventional two-dimensional media, and the same principle will apply when the same content is visualized by three-dimensional, augmented means. Even though augmented images are not actually in the physical environments in which they are made to appear, they nevertheless reside in a digital intermediary that is sufficiently "tangible" – such as on the lens of a head-mounted mobile device or in a cloud-based computer server. The "tangible fixation" element requires only that the works be stored in a media "from which they can be perceived, reproduced, or otherwise communicat-

ed, either directly or with the aid of a machine or device."[47] The specific type of device used to perceive the content is irrelevant.

A decision issued in September 2013 by the U.S. District Court for the Southern District of New York gives a preview of how AR copyright cases are likely to look. In *Firesabre Consulting LLC v. Sheehy*,[48] middle school technology teacher Cindy Sheehy purchased a set of islands within the virtual world *Second Life* for use in teaching students. Each island in the simulation starts off as a flat green rectangle, and the user can then change the topography and landscape of the island (known as "terraforming") using a series of interactive tools provided by Linden. Firesabre – a consulting firm specializing in the educational use of virtual worlds – performed various terraforming services for Sheehy on those islands, including a train station, a café, music shops, and a volcano. When the relationship between the parties broke down, Firesabre claimed copyright ownership in all of the terraformed content. Allegedly, Sheehy continued to display the content within *Second Life* and copied some of it to another virtual world, all of which Firesabre asserted to be copyright infringement.

The court denied Sheehy's motion for judgment as a matter of law, holding instead that Firesabre had alleged plausible allegations of infringement. First, the court decided that the works had been "fixed in a tangible medium" because they existed on Linden's data servers and were visible within *Second Life* for a sufficient period of time to be perceived by the students who interacted with the islands.

Second, the court saw no reason to deny copyright protection to the terraformed works simply because others could come along later and modify them. "In this regard," the judge wrote, "I see no distinction between the terraforming designs and a drawing created on a chalkboard or a sculpture created out of moldable clay. That someone else could come along and, with or without permission, alter the original piece of art does not mean the art was too transitory to be copyrighted in the first place."[49] Therefore, even dynamic AR content will spark copyright law controversies.

### Originality and the idea/expression dichotomy
Not every expressive work is automatically eligible for copyright protection. Both the U.S. Constitution and the Copyright Act require that the expression within the work be original to its author.[50] Originality is therefore said to be the "*sine qua non* of copyright." As explained by the

45   17 USC §102 (2012)
46   For example, "all portions of [a video game] program, once stored in memory devices anywhere in the game, are fixed in a tangible medium." Stern Elecs., Inc. v. Kaufman, 669 F.2d 852, 855 n.4 (2d Cir. 1982)
47   17 USC §102 (2012)
48   Firesabre Consulting LLC v. Sheehy, No. 11-CV-4719 (CS), 2013 WL 4520977 (S.D.N.Y. September 26, 2013)
49   Id.
50   See Feist Pub'lns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 346 (1991); 17 U.S.C. § 102 (2012)

U.S. Supreme Court, the word "original" in this context does not mean novelty (as is required by patent law), but rather that the work was independently created by the author as opposed to copied from other works, and that it possessed at least some minimal degree of creativity.[51] The author "must have made some contribution to the work which is irreducibly his own."[52]

A copyright is not a reward for mere effort or toil. A work that merely copies or compiles facts or the expression of others – no matter how much skill and effort that copying or compilation may require – cannot be copyrighted. This "idea/expression dichotomy" is the heart and soul of copyright law. That does not mean, however, that the expression must have any degree of artistic or aesthetic merit. As the U.S. Supreme Court held more than a hundred years ago, even "a very modest grade of art has in it something irreducible, which is one man's alone. That something he may copyright."[53] All that is needed is some creative spark, "no matter how crude, humble, or obvious."[54]

The application of these principles to augmented reality were foreshadowed in the 2008 case *Meshwerks v. Toyota Motors Sales USA, Inc*.,[55] which applied the age-old principle of originality to the relatively new technology: digital modeling (Figure 9). In 2003, Toyota and its marketing partners decided to begin creating digital models of Toyota's vehicles for use on Toyota's website and in various other media. This approach offered significant cost savings over the prior method of obtaining vehicle images, which required a new photo shoot of entire fleets of vehicles each time even the smallest design element changed. Digital images, by contrast, can be edited with a few mouse clicks.

Toyota's marketing partners subcontracted with a company called Meshwerks to conduct the first two initial steps of the project – digitization and modeling. Meshwerks began this process by collecting hundreds of physical data points from the vehicles to be portrayed. Based on these measurements, modeling software (such as Maya) generated a digital "wire frame" image. Meshwerks personnel then finetuned the lines on screen to resemble each vehicle as closely as possible. According to Meshwerks, approximately 90 percent of the data points contained in each final model were adjusted by a person. Some areas of detail – including the wheels, headlights, door handles, and Toyota emblem – could not be mechanically measured and instead were added by hand.

When Toyota and its partners later used these wire frame images in ways to which Meshwerks objected, Meshwerks sued, claiming that it owned a copyright in the images. Both the district court and the court of appeals, however, disagreed, holding that the wire frame models were merely copies of Toyota's products, and not sufficiently original to warrant copyright protection. The courts stressed that, despite the significant amount of effort Meshwerks invested in creating the images, it had never
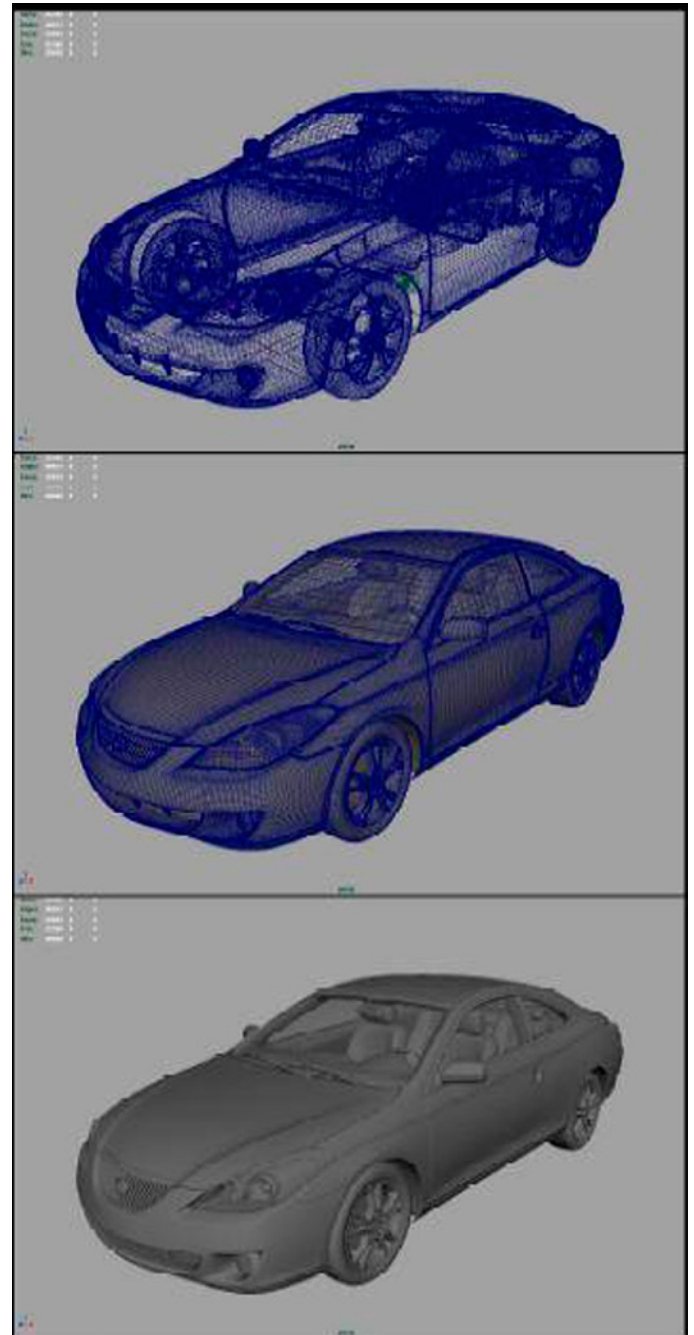


*Figure 9.* The digital wireframes at issue in Meshwerks v. Toyota Motors Sales USA, Inc

51 Feist Pubs., Inc. v. Rural Tel. Serv. Co., Inc., 499 U.S. 340, 345-46 (1991)
52 Todd v. Montana Silversmiths, Inc., 379 F. Supp. 2d 1110, 1112 (D. Colo. 2005)
53 Bleistein v. Donaldson Lithographing Co., 188 U.S. 239, 250 (1903)
54 Feist, 499 U.S. at 345
55 Meshwerks v. Toyota Motors Sales USA, Inc. 528 F. 3d 1258 (10th Cir. 2008)

intended to create something original. To the contrary, its express intention was to replicate, as exactly as possible, the image of certain Toyota vehicles. That is the only way in which the images would have been useful to Toyota as substitutes for photographs of real vehicles.

Several other courts have likewise denied copyright protection in analogous cases, involving digital copies of physical facts and prior works of art. For example, in *Sparaco v. Lawler, Matusky, Skelly, Engineers LLP*,[56] the court denied copyright protection to the elements of an architectural drawing that conveyed "the existing physical characteristics of the site, including its shape and dimensions, the grade contours, and the location of existing elements, [because this portion] sets forth facts, [and] copyright does not bar the copying of such facts."[57] Other cases have denied copyright protection to catalog illustrations of transmission parts "copied from photographs cut out of competitors' catalogs,"[58] and to high-quality photocopies of paintings.[59] They have also denied protection to other examples of the "dimensional shifting" that Meshwerks did replicating a three-dimensional object in two dimensions. For example, courts have held that three-dimensional plastic toys[60] and costumes[61] based on pre-existing, two-dimensional cartoon characters were not original.

Anticipating the negative reaction to its decision that did, in fact, come from several sources, the *Meshwerks* court went out of its way to stress that "[d]igital modeling can be, surely is being, and no doubt increasingly will be used to create copyrightable expressions."[62] It even suggested "that digital models can be devised of Toyota cars with copyrightable features, whether by virtue of unique shading, lighting, angle, background scene, or other choices. The problem for Meshwerks in this particular case is simply that the uncontested facts reveal that it wasn't involved in any such process, and indeed contracted to provide completely unadorned digital replicas of Toyota vehicles in a two-dimensional space."[63]

Another example of the same issue is the recreation of real people. This is not hypothetical; there are already several companies publishing or working on augmented entertainment content that involves the replication of actual celebrities and historical figures. To the extent that these "characters" merely replicate the attributes of an actual person, they will not contain original, copyrightable content.

These cases illustrate the fine line between originality and reproduction for digital imitations of reality. Because

AR content is meant to be perceived in conjunction with physical objects – often in a manner intended to create the illusion that the digital content is itself physical – we will be more likely to find digital content that straddles this line in AR than we are in other digital contexts. This will be increasingly true as the technology improves, creating higher-resolution images and more stable displays. (The fact that eligibility for copyright protection would decrease as the quality of the image increases understandably strikes some as a perverse result, but it is entirely consistent with the purposes of copyright law, as courts have repeatedly explained.) This could result in augmented environments that intentionally bear slight, digitized differences from their real-life inspirations – such as, for example, the flora and buildings in the Second Life islands in the *Firesabre* case – solely for the purpose of preserving original expression and therefore copyright protection. In other cases, though, it will simply mean that content creators will need to rely on other compensation models to reward them for their effort.

There may also come a day when augmented digital objects are so utilitarian that we come to think of them as functional tools rather than expressive works. Consider, for example, the menu layouts of most word processing programs, or the graphics used to symbolize such functions as "power on/off," "play," and "pause." If there were only one software program in existence that employed these arrangements and graphical works, they may well be considered copyrightable. In reality, however, they merely represent methods of organization that are commonplace and critical to the function of thousands of programs. Although there is some room for minute variations in how these user interfaces are expressed, that room is so narrow that such variances will not be considered sufficiently original for copyright protection. (This is what copyright law calls the "merger doctrine." Both it and a related doctrine known as *scenes a faire,* or scenes that must be done, describes elements of an expression that are so common to its genre that they can no longer be considered original.) In an augmented world, we may come to rely on all sorts of augmented user interface designs that then become standardized *scenes a faire*, thereby depriving them of the ability to be protected by copyright.

## REPRODUCTION AND DERIVATIVE WORKS
The foregoing section imagined augmented environments so similar to real-world objects that they cannot be protected by copyright. Much more frequently, however, augmented expression will reproduce other, pre-existing creative works – and therefore infringe their copyrights.

56  Sparaco v. Lawler, Matusky, Skelly, Engineers LLP, 303 F.3d 460, 467 (2d Cir. 2002)
57  Id. at 467
58  ATC Distr. Group, Inc. v. Whatever It Takes Transmissions & Parts, Inc., 402 F.3d 700, 712 (6th Cir. 2005)
59  Bridgeman Art Library, Ltd. v. Corel Corp., 36 F.Supp.2d 191, 197 (S.D.N.Y. 1999)
60  Durham Indus., Inc. v. Tomy Corp., 630 F.2d 905, 910 (2d Cir. 1980)
61  Entm't Research Group, Inc. v. Genesis Creative Group, Inc., 122 F.3d 1211, 1221-24 (9th Cir. 1997)
62  Meshwerks v. Toyota Motors Sales USA, Inc., 528 F. 3d 1258, 1269 (10th Cir. 2008)
63  Id. at 1269-70

## Duplicating copyrighted works

In order to prove infringement, a copyright owner must show a "substantial similarity" between the copyrightable expression in the two works. When one work entirely copies another that is an easy showing to make. Because so many AR applications will rely on video technology – particularly wearable devices with video recording capability – replicating copyrighted expression will always be a concern. After all, before digital eyewear is able to add digital content to our view of the world, the devices must first be able to know what we're looking at.

One of the earliest examples of this concern occurred on January 18, 2014 in Columbus, Ohio. That's when Federal agents from the Department of Homeland Security and local law enforcement officials allegedly yanked a customer out of a movie at AMC Theaters and interrogated him for several hours. His crime? Wearing Google Glass in a movie theater. The moviegoer was released only after demonstrating that he had not activated the recording function of the device during the film.[64]

Of course, this concern is by no means unique to wearable technology. In all likelihood, more than 90% of the other patrons in the theater were carrying smartphones, any one of which had both video recording capability *and* enough battery power to last throughout the film – something Glass definitely does *not* have. There was no word on how many of them were interrogated. Nevertheless, the emerging revolution in wearable and Internet of Things technologies will certainly multiply the number of recording devices in the wild, and with that will come concerns that copyrighted works are being reproduced.

Other exact replicas of copyrighted works may be deliberate. In order to create an immersive augmented experience of a far-away place, for example – as some companies are already contemplating – the location will need to be exactly duplicated. That would likely include any copyrighted artwork that may be visible in the scene.

Even transferring a work from one medium to another, without more, is a mere reproduction (and hence infringement) of the copyrighted expression in the original. In *Meshwerks*, the thing being copied was not a copyrighted work, so the only consequence of this copying was that the new work lacked originality. Where the thing being copied is copyrighted, however, the reproduction is an infringement of that copyright. A U.S. Court of Appeals reached a very similar conclusion in *Gaylord v. United States*.[65] There, the U.S. Postal Service issued a (two-dimensional) stamp depicting the (three-dimensional)

Korean War Veterans Memorial in D.C. The creator of that sculpture successfully argued that the stamp merely copied his expression and reproduced it in a different medium.

Many artists will see AR as a medium in which they can "bring to life" existing works, especially those that currently only exist in two dimensions. If they are not careful to add their own expression to those recreations, however, a court may find them to be mere reproductions – infringements – of the copyright in the existing work.

## Adding to existing works

Substantial similarity becomes more challenging to demonstrate when the copies are not exact. "[T]he copying [must be] quantitatively and qualitatively sufficient to support the legal conclusion that infringement (actionable copying) has occurred. The qualitative component concerns the copying of expression, rather than [non-protectable elements].... The quantitative component … must be more than '*de minimis*.'[66] Neither threshold is particularly high, but it is ultimately a subjective determination by the court.

The exclusive right to make "derivative works" is closely related to the idea of making an inexact, but substantially similar, reproduction. A derivative work is simply the addition of new expression to an existing work. In either case, a substantial portion of the original work exists in the new one, and the copyright owner's rights have been infringed.

Since the very definition of "augment" is "to make greater," augmented reality tools carry with them an inherent risk of creating derivative works. In its most straightforward form, visual AR involves overlaying digital data on top of physical things in order to add content to it or change its appearance.

A few examples capture the point:

- In the books *Daemon* and *Freedom™* by Daniel Suarez, a character nicknamed "The Burning Man" is memorialized by a statue. To the naked eye, it appears to be a conventional sculpture. Viewed through AR glasses, however, it become wreathed in three-dimensional flames, and studded with links to videos and tributes.
- As part of their 2011 Re + Public collaboration, the Heavy Projects and the Public Ad Campaign used AR to "filter" outdoor advertising and replace it with original street art. Looking through an AR app, outdoor commercial advertisements were overlaid with political or artistic messages. One such pointed message caused the image of "Captain Barbossa" in the poster for *Pirates of the Caribbean 4* to morph before a user's eyes into the face of Goldman Sachs CEO Lloyd

64  Julie Streitelmeier, AMC movie theater calls 'federal agents' to arrest a Google Glass user, The Gadgeteer (January 20, 2014) http://the-gadgeteer.com/2014/01/20/amc-movie-theater-calls-fbi-to- arrest-a-google-glass-user/
65  Gaylord v. United States, 595 F. 3d 1364 (Fed. Cir. 2010)

66  Castle Rock Entm't v. Carol Publ'g Grp., 150 F. 3d 132, 138 (2d Cir. 1998)

Blankfein conveying the artist's message that he is the "real pirate" (Figure 10). Similar projects have superimposed digital content onto public murals in a form of augmented graffiti.

- Artist Amir Baradaran published a mobile app called "Italicizing Mona Lisa." It is designed to display on your phone as you hold it up to a physical version of the iconic painting, creating the video illusion that the woman depicted there wraps herself in the Italian flag.

- "Projection mapping" uses three-dimensional video to animate stationary objects, usually the sides of buildings. When done well, projection mapping creates the powerful illusion of a building actually coming to life and moving in three dimensions.

Do these digital animations infringe the copyright of the physical art they augment? In the typical "augmented substitution" scenario, in which content on a mobile screen simply overlays or complements the existing



**Figure 10.** *From Pirates of the Caribbean to "the Real Pirate."*

work, no infringement is likely. That is because the digital content is not actually doing anything to the original work. It is not making a copy of or altering the original. Even though the physical display acts as a trigger for the digital content, and even though the user's mobile device causes the digital content to appear as if it exists in the real world in place of the original, it doesn't actually exist there. It's an effective illusion for creating an immersive experience, but it's an illusion nonetheless. The content stays on the mobile screen, where it is a separate digital work that exists apart from the physical display.

But the question gets more complicated when the digital content actually makes the physical display appear to morph, as in the *Pirates of the Caribbean* and *Mona Lisa* examples. That is because, more likely than not, the AR software has already stored a reference copy of the original and altered versions of the physical work. In other

words, the programmer may have created a reproduction and a derivative of the physical work long before anyone uses the program to interact with the physical artwork. In order to create the illusion of movement in the physical painting, the AR programmer first reproduced the artwork, then created a digital alteration of it. That doesn't raise any copyright concerns with public domain works like the Mona Lisa, but artists who digitally copy and morph copyrighted works are taking a risk.

## Augmented architecture

Projection mapping and other means of augmenting architectural works add another layer of nuance. Today, this technology is confined to elaborate, after-dark advertisements on the sides of buildings. After AR becomes ubiquitous, however, I doubt that there will be many buildings that are not animated in one way or another. Unlike contemporary projection mapping, the effect will be superimposed by the user's AR viewer, instead of light being physically projected onto the surface of the building. Those who design these experiences will no longer be limited to the actual physical dimensions of the brick-and-mortar edifice. Instead, you could find a building actually wrapping its (simulated) arms around you, or see (virtual) flames spewing from its windows, or any other effect one can imagine. All of which leads a curious IP attorney to wonder: could any of this activity infringe the architectural copyrights of the person who designed the building?

One type of creative expression in which copyright may inhere is an "architectural work"–i.e., "the design of a building as embodied in any tangible medium of expression, including a building, architectural plans, or drawings."[67] But Congress also recognized that allowing architects to fully enforce all five of the basic copyright rights could cause all manner of logistical nightmares throughout society. So it pared back some of the protections available in architectural works. Specifically, Section 120 of the Copyright Act[68] allows people to make, distribute, and display pictures of public buildings. It also lets the owners of a building alter or destroy the building, if they so choose, without needing to first get the architect's permission.

With these things in mind, let's consider whether projection mapping impermissibly adapts (or, in copyright parlance, "creates a derivative work of") the architectural work embodied in the building being projected upon.

The short answer, in my view, is "no." With the caveat, the outcome of any particular case depends on the specific facts at issue. It is difficult to imagine a realistic scenario in which projection mapping (as it's currently

67  *17 USC §101 (2012)*
68  *17 U.S.C. § 120 (2012)*

done) would create an infringing derivative work. At least two reasons come to mind. First, nothing is actually being done to the architectural work (i.e., the building design) itself. Instead, the presentation involves two separate "works"–the building, and the video. Yes, the video is designed to take advantage of the unique design of the specific building that it's being projected upon. Its effect would be far less impressive if it were projected onto any other surface. And that effect is meant to create the illusion that the building design is changing. But it's only an illusion. No actual alteration to the architectural work ever occurs.

Second, even if a creative litigation attorney argued that simply creating the perception of a morphing building was enough to create a derivative of the building design, such an "alteration" should fall within Section 1209s exception. Although there is very little case law interpreting Section 120, one court accurately observed that "Section 120(b) does not expressly contain any limitation upon the manner or means by which a [building owner] may exercise his right to alter the structure. Presumably, no such limitations were intended by Congress, else they would be expressed in [that section]."[69] The one catch here is that, as written, this statutory exception allows only the "owner" of a building, not anyone else, to authorize an alteration to the building. So the projection mappers would need to have the owner's permission; guerilla marketers would not have this statutory defense. Again, though, there would not appear to be any actual alteration made in the first place.

But would the result be the same if the illusion of an animated building were accomplished through AR smartphone/eyewear instead of an actual video presentation? Yes–for the most part. Whether the video image is actually projected on a building or only overlaid over the viewer's perception via AR, there is still no alteration of the actual building occurring.

There is a potential catch, however, depending on how the AR effect is accomplished. If the data superimposed on the building consists solely of original imagery designed to overlay the building, that's conceptually equivalent to existing projection mapping. But what if the AR designer copies the actual building design into virtual space, then alters that design, in order to create the end result? That would complicate things from a copyright perspective. An architectural work can be embodied either in 2-D written drawings or in a 3-D manifestation. Making a copy of the design is infringement, unless an exception applies. Section 120 allows people to make "pictures, paintings, photographs, or other pictorial representations of the work." A virtual recreation may very well fit that descrip-

tion. But the statute does not expressly allow the person who makes that pictorial representation to then alter the picture. Arguably, that could be creating a derivative work.

Even under those circumstances, potential defenses are available. For example, at least one court[70] has found within Section 120 an implied right to copy and alter a building's plans for the purpose of creating an owner-approved alteration to the building. Otherwise, the court reasoned, an architect hired by a homeowner to renovate a home would be forced to do so without the benefit of written plans–a dangerous prospect. A similar argument could be made in the AR space, depending on the purpose of the alteration. A different court,[71] however, has disagreed that any such implied right to copy plans for the purpose of altering a building exists.

## PUBLIC DISPLAY AND PERFORMANCE

Public display and performance rights will also be at issue, in sometimes novel ways. Because most AR content will be experienced through individual mobile devices, one might presume those experiences to be private, rather than public, displays and performances. But AR programs that are aware of a user's geolocation and that are designed to portray content as being physically manifest at that location challenge that presumption. For example, the British Museum released a mobile app designed to show users historical London photos in the actual, public location where they were taken. The photo itself never leaves the confines of the mobile device, but its display is triggered by the user's physical location.

The same issue is presented by performances of location-aware video content. In 2011, tech news outlets reported on a man who had tattooed on his arm a target marker image used by a Nintendo 3DS game to represent an animated dragon. To the outside world, the tattoo was simply an uninteresting, approximately square-shaped symbol. When viewed through the 3DS device, however, it came to life as a threedimensional, moving dragon.

Is that a "public" display and performance? And if so, has the app developer or end user acquired from the copyright owner the appropriate license rights for that public display? The case of the dragon tattoo seems likely to have exceeded whatever license may have come with the 3DS device for displaying the content. Entire industries were forced to confront the limitations of their licenses when the internet became a new medium for republishing old content; AR will present similar challenges. User-generated content and social media will guarantee that works get publicly displayed in all sorts of unanticipated ways.

69  Javelin Investments, LLC v McGinnis, CA H-05-3379, 2007 US Dist Lexis 21472 (S.D. Tex. January 23, 2007)

70  Id.
71  Guillot-Vogt Associates, Inc. v. Holly & Smith, 848 F.Supp. 682 (E.D. La. 1994)

Such questions will grow in importance as our surroundings become populated with triggers for all sorts of digital data.

## MORAL RIGHTS

The collection of rights known as "moral rights" are quasi-copyright protections entitling the creator of an artistic work to protect the integrity of their creation, regardless of who may come to own the work. This is primarily a European concept not recognized in U.S. law, and therefore is beyond the scope of this book. A form of moral rights, however, can be found in the Visual Artists Rights Act, which, among other things, gives artists a limited right "to prevent any intentional distortion, mutilation, or other modification of that work which would be prejudicial to his or her honor or reputation."[72]

Whether the VARA or similar rights will ever apply to AR content remains to be seen. Case law interpreting this right is scarce, and by its very nature it cuts against the grain of the Copyright Act's design. United States copyright law places the power to control a work in the hands of whomever owns its copyright, as opposed to the original artist who created the work and then only within the five exclusive rights of a copyright holder. Moreover, digital augmentations of a physical work typically will not alter the actual physical work. Nevertheless, the foregoing *Mona Lisa* example illustrates how convincingly a physical work of art can digitally be made to appear as if it is being distorted. It is easy to foresee a visual artist taking umbrage to such augmentation, and resorting to every creative legal means available to enjoin it.

## FAIR USE

Each of the foregoing examples of scenarios that may be considered copyright infringement are subject to affirmative defenses that may defeat the claim under particular circumstances. Among those is the defense of fair use. The Copyright Act identifies certain activities that are presumptively permissible under this doctrine – including "criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research."[73] This list of preferred activities derives directly from First Amendment case law, as each of these is an example of speech that contributes in one way or another to conversation about issues of public importance. It is a recognition that free speech rights ought to trump intellectual property protections in some circumstances.

Unlike most statutory exceptions to copyright infringement liability, however, whether any particular use is "fair" under any given set of circumstances can only be determined on a case-by-case basis by applying four subjective principles:

1. The purpose and character of the use, including whether such use is of a commercial nature or is for non-profit educational purposes;
2. The nature of the copyrighted work;
3. The amount and substantiality of the portion used in relation to the copyrighted work as a whole; and
4. The effect of the use upon the potential market for or value of the copyrighted work. [74]

In practice, most fair use cases center on the first and fourth factors. Many courts tend to cast the first factor in terms of whether or not the challenged use somehow "transforms" the purpose or character of the original work. Some of the foregoing examples, such as the augmentation of the *Pirates of the Caribbean* poster, have an obvious political message, which is a presumptively preferred "purpose and character" of use. Another popular (although not always successful) line of argument is that a use "transforms" the original by "mashing" it up in a display with multiple other works. For example, *Cariou v. Prince*[75] involved relatively crude and simplistic physical augmentations made to photographs. The iconic example from that case involved a guitar and psychedelic face mask that the defendant slapped on top of the photo of a Jamaican man. The Second Circuit held that even these simple additions were sufficient to fairly transform the original. Similarly, in June 2014, the Second Circuit held that Google's massive project to scan books into an enormous, searchable database was a fair, "transformative" use of the books because the originals were not capable of being searched. If these decisions hold as precedent for future cases, they could open the door to all manner of digital augmentations to other works.

The fourth factor – which assesses the impact of the defendant's work on the original's commercial value – will be difficult to ascertain, especially in early cases. The medium of AR is so nascent, and there are so few business models based on it, that there will be very few reliable facts from which a court can draw a conclusion. This uncertainty will cut both ways. In some cases, the lack of evidence will lead a court to conclude that there is no market for the original in the AR medium. Other courts, however, will reach the opposite conclusion, afraid that the defendant's use will have foreclosed the plaintiff's ability to exploit the limitless possibilities available for creating value in this yet-to-be-defined market.

The most significant drawback of the fair use defense is always its uncertainty. Someone proposing to use another's copyright work without permission cannot reliably

72  17 USC 106A (2012)
73  17 USC 107 (2012)

74  17 USC 107 (2012)
75  Cariou v. Prince, 714 F.3d 694 (2d Cir. April 25, 2013)

determine ahead of time whether the use is fair; instead, the decision may only be made by a judge or jury in response to a copyright infringement lawsuit. Therefore, although fair use is commonly invoked to justify all manner of uses, it is never a reliable safeguard.

## AUGMENTED COPYRIGHT ENFORCEMENT

Copyright enforcement will also be a major challenge in the AR medium. The mass lawsuits of the past two decades against file-sharers and signal pirates have required a significant amount of detective work and discovery to connect individual users to allegedly infringing downloads. Pursuing legal action against those who share infringing content in the augmented medium will not differ categorically from these efforts. After all, augmented content only *appears* to exist in three dimensions; in reality, it will still reside in a hard drive, device, or server somewhere that can be located and tracked. Indeed, the earliest versions of digital eyewear available now have relatively little on-board memory or processing power, and only connect to the internet by means of a connection (some hard-wired, some wireless) to a mobile phone, and many of their apps reside in the cloud.

As augmented content proliferates across the Internet of Things – and especially the types of distributed, *ad hoc* mesh networks described in Chapter 2 – the substance and sources of data will become that much harder to track. The entire world will eventually become a giant peer-to-peer sharing network; think of AR channels as bit torrent sites that users can walk through, see, and touch. So-called "darknets" – sealed digital communities with no visible connection to the internet – will become much more common.

One can imagine that it will become even more difficult to prove that a particular user viewed a particular work when the "display" occurred entirely within a mobile headset. As discussed in Chapter 10, I expect that many litigators will soon be conducting "v-discovery," in which they must determine not only the device to which virtual data was routed, but also where individual users were located, and in what direction they were looking, when the data was displayed.

On the other hand, AR eyewear could also be used as a copyright *enforcement* mechanism. The YouTube video *A Read-Only Future*[76] depicts life through the eyes of someone wearing digital eyewear that is regulated by the entertainment industry (Figure 11). His glasses recognize copyrighted content in the user's field of view or range of hearing – such as a photo hanging on the wall or a song being played on the sidewalk – and obscures it unless he agrees to a micro-license payment. Just as in

concept videos for actual digital headsets, the eyewear in this video is able to share content directly to Facebook, but these will refuse to do so if they detect unlicensed content. They even alert the authorities if the user stumbles across an unauthorized reproduction published by someone else. Excerpts from copyright skeptic Larry Lessig feature prominently in *A Read-Only Future*, which plays out as if it was Lessig's nightmare.

This scenario is entirely plausible in light of how most AR apps function today. A mobile device scans the ambient world looking for one of the targets it is preprogrammed to recognize. Each time it captures a view, the device sends that image to the cloud to check against the portfolio of targets. If a match is found, the cloud server sends back the digital content associated with that target. Several non-AR apps operate in a similar way; for example, the popular mobile app Shazam listens to ambient music and identifies it in real time, allowing users to purchase a copy of the song or follow along to the lyrics.
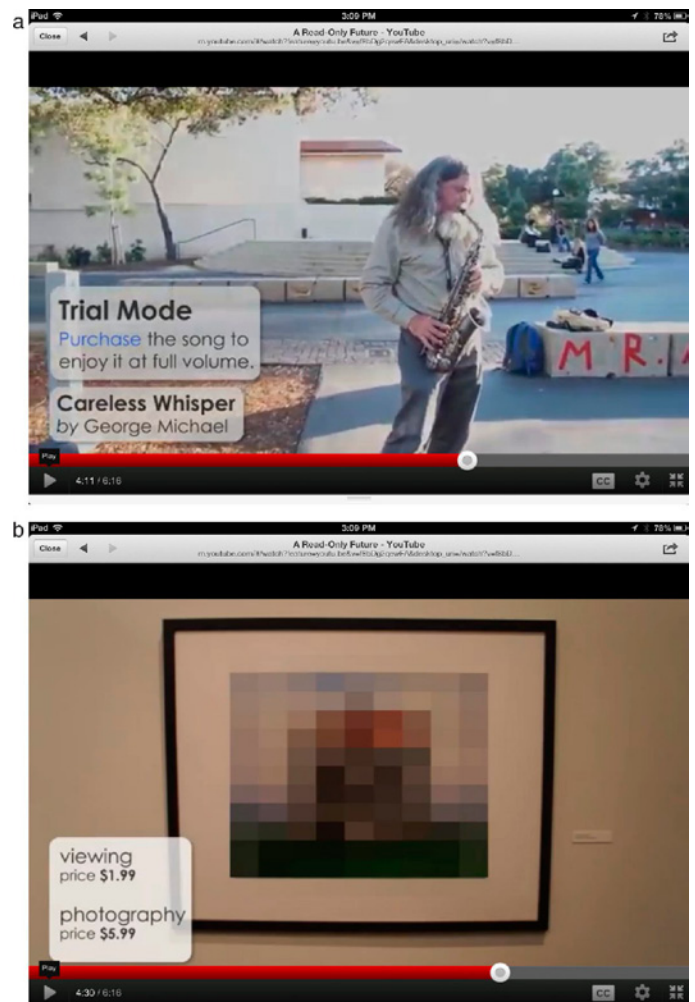
**Figure 11.** *Excerpts from A Read-Only Future*

76  A Read-Only Future, Youtube (March 16, 2013) https://www.youtube.com/watch?v=f8bDg2qewFA

A few months before this book went to print, Shazam became available on Glass.

It would be child's play to simply add a roster of copyrighted works to a cloudbased catalog of targets. Every time the cloud server recognizes one of the protected files in its database, it could be set to trigger a request for micropayment, or obscure the work, or even issue a warning to law enforcement or the copyright owner itself. The fine print in our mobile app stores already prohibits us from using the apps to commit copyright infringement; this would be going one step further to turn mobile devices into the eyes and ears of the copyright police.

Such an enforcement mechanism could potentially be so effective, and offer such a unique functionality not available by any other means, that the company able to provide it would be foolish not to monetize it. Today, mobile devices (including digital eyewear) receive their internet connections through such providers as AT&T, Verizon, Sprint, and the like. In the near future, we may instead get online directly through the "panternet" mass wireless signals emitted by Google or Facebook and discussed in Chapter 2. Whichever company provides that service could easily sell to copyright owners the ability to police copyright compliance through the network of AR-capable devices they serve. Internet service providers (ISPs) would then become analogous to the performance rights organizations (PROs) of today – ASCAP, BMI, and SESAC – which rely on human investigators to overhear unlicensed public performances of copyrighted music. Indeed, these PROs could contract directly with ISPs to enforce their entire catalogs – deputizing every AR app user as investigators.

With such an arrangement in place, ISPs might even share the wealth in order to incentivize users to cooperate. Imagine if AR users received a micropayment each time they used their device to report an observed copyright infringement. Knowing that anyone you meet is a potential copyright cop would certainly be a powerful disincentive to would-be casual infringers. Five years from now, instead of movie theaters detaining and interrogating digital eyewear users, they may be rewarding them.

## LICENSING

As with anything else, copyrights can be enforced through either carrots or sticks (or a combination of the two). If the aggressive enforcement action described above is the stick, then the carrot would be offering licensed content. In the early 2000s, digital music piracy was rampant, and CD sales were in free-fall. Not because the internet and digital music were inherently unlawful, but because the traditional publishers of copyrighted music offered no satisfactory

alternative to meet the demand for digital music. Not until Apple introduced iTunes in 2003 did consumers finally have a digital marketplace robust enough to meet their needs. Since then, digital distribution (through iTunes, more often than not) has become the default means of obtaining new music.

It remains to be seen how much of a problem copyright piracy will be in the AR medium. Establishing an infrastructure for lawfully obtaining a wide variety of desirable content, however, will still be the means by which content creators will be able to make money from AR. In October 2013, NYU Polytechnic professor Mark Skwarek (who also created the "Leak in Your Home Town" app described in the foregoing trademark discussion) introduced the first augmented Halloween masks (Figure 12).[77] Trick-
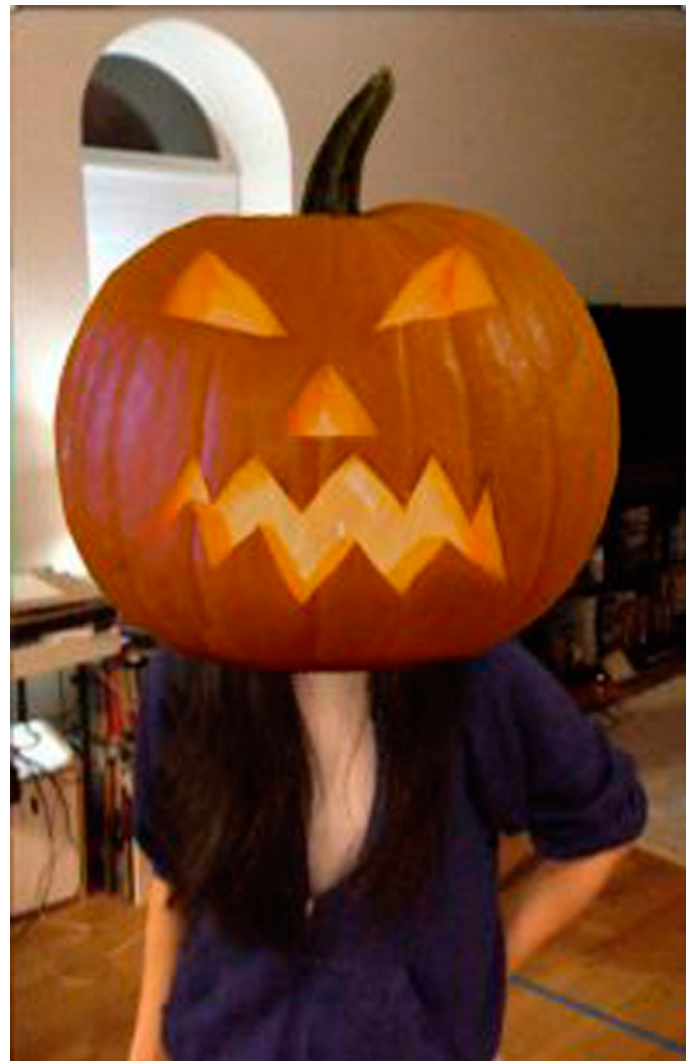


**Figure 12.** *Prof. Mark Skwarek's Augmented Halloween Mask*

77   Mark Skwarek, Still Wearing a Real Mask this Halloween?, Polytechnic School of Engineering (October 28, 2013) https://engineering.nyu.edu/press-release/2013/10/28/still-wearing-real-mask- halloween

or-treaters wearing a four-inch target in their hat or hair would be seen by users of Skwarek's AR app as if they were wearing giant, virtual masks. Once enough devices are in place to make the ability to perceive such content sufficiently ubiquitous, companies could easily begin selling entire lines of virtual Halloween costumes. The same infrastructure would allow sales of augmented clothing year-round, along with augmented ornaments, décor, signage, toys, games indeed, a digital analog of almost anything that exists physically.

Copyright owners could also license the right to make particular uses of augmented content. Today, for example, owners of musical works sell "sync" or "soundtrack" licenses to filmmakers, which convey the right to "sync" a particular song with video content into an audio-visual film. There is no logical reason why copyright owners could not likewise license the ability to sync their works with any physical object via the augmented medium. Want passersby to see a copyrighted dragon image on your arm (as in the foregoing example of the man with the tattoo of a Nintendo 3DS marker)? Pay the license fee. Are you a University of Michigan fan and you want other drivers (using augmented windshields) to see your car as if it were a giant, blue-and-maize-wearing wolverine? Pay the license fee. Want to see Mickey Mouse ears on the moon each time it rises? The list of examples is limited only by one's imagination.

On today's internet, copyright enforcement blends with licensing in the form of paywalls – websites that cannot be accessed without making a micropayment or purchasing a subscription. When it comes to augmented content, we could easily encounter similar paywalls – including some that we perceive as actual, physical walls – literally everywhere we go. Digital entertainment and other content could be made available floating in mid-air, on the side of a building, or anywhere else – but only accessible for a micropayment. As discussed earlier, the infrastructure for such payments is already being constructed. In 2013, Google obtained a patent for "pay per gaze" and "pay per emotion" systems. Although these are described as methods for ISPs to charge advertisers based on a consumer's reaction to the ad, the concept could just as easily be adapted to take payments from consumers in order to access the advertising or other content. Chapter 4 described multiple ways in which companies are already beginning to explore such "commARce" solutions.

Of course, too much reliance on such business models could have adverse social consequences. Retailers have always known the power of "impulse purchases," as well as how to position and price their content attractively enough to entice users to buy. It is a profitable model for retailers, but not exactly conducive to consumers maintaining a disciplined budget. If large quantities of copyrighted content

– news reports, public art, television shows, and the like – became available only behind AR paywalls, it could deprive society as a whole of valuable experiences and encourage excessive spending. At this point, however, these remain only long-term, hypothetical concerns. How the new economic models shake out remains to be seen.

## THE RIGHT OF PUBLICITY

Just as trademarked objects can easily serve as triggers for digital content, so too can the physical characteristics of individual people. The simmering debate over facial recognition technology and privacy summarized in Chapter 3 is a preview of the concerns we are likely to face when a large segment of the population is wearing eyewear capable of recognizing the faces of others.

The main concern voiced about this technology to date has been "privacy," although society in general seems to have no consensus about what that word actually means. But I also expect that the right of publicity – that weird, state-law transitional species between the common law of privacy and intellectual property – will play an increasingly prominent role in this debate going forward.

## THE BASICS OF PUBLICITY RIGHTS

The right of publicity is a state-law right that emerged from the common law of privacy to become more or less recognized as a form of intellectual property. It is the fourth of Dean Prosser's four causes of action for invasion of privacy discussed in Chapter 3. Although the particulars vary slightly from state to state, it is essentially the right of an individual to control the commercial exploitation of his or her likeness. The best summary of the right of publicity as generally understood across the United States comes from the *Restatement (Third) of Unfair Competition* section 46: "[o]ne who appropriates the commercial value of a person's identity by using without consent the person's name, likeness, or other indicia of identity for purposes of trade is subject to liability." Each clause of this definition holds legal significance.

### Commercial value
The "commercial" aspect of this right is intentional. It is what distinguishes the use of someone's likeness in creative expression like a movie or song – which is generally free speech privileged by the First Amendment – from commercial speech designed to advertise and sell goods or services, which is more akin to a trademark, and hence within the realm of governmental regulation and property rights. In order to prevail on a publicity rights claim, therefore, a plaintiff must generally prove that her identity has "commercial value" – i.e., that there is reason to believe

that her identity would be worth something to an advertiser, or that a customer might be more likely to pay attention to a product because the plaintiff's identity was associated with it.

For that reason, courts had long ruled that the right of publicity was only available to "celebrities," and not the rest of us. Today, the rise of digital (and especially social) media makes it entirely realistic to argue that we can all attain commercial value in some context. One argument for establishing "commercial value" in social media is the value of personal relationships. On many social media sites, the identity of the person with whom one interacts in social media both incentivizes people to participate in the site and adds qualitatively significant value to the experience. And the more such interactions that occur on a particular social media site, the more benefit the owner of that site derives (in terms of advertising revenue, search engine tie-ins, or whatever the site's business model may be).

Therefore, in a very direct and measurable way, some would argue, digital (and especially social) media is a context in which literally every user's identity has potential commercial value. Two judicial decisions stemming from lawsuits filed against Facebook in recent years have given some credence to this view,[78] as did a lawsuit over a banking executive's LinkedIn profile.[79]

### Likeness

In this context, one's "likeness" typically takes the form of one's physical appearance, name, signature, or voice. The restatement expressly lists two examples of ways in which a person's identity can be "indicated": their "name" (which typically includes both the name itself and the person's signature) and their "likeness," or personal appearance. But the common law includes in that term any other "indicia of identity." So a famous race car driver's likeness was infringed by using a picture of his distinctive car, and Johnny Carson's right of publicity was infringed by the product name "Here's Johnny Portable Toilets" because the phrase "Here's Johnny" had come to be associated with Carson.

### FACIAL RECOGNITION AS INFRINGING THE RIGHT OF PUBLICITY

Before long, someone is going to file a lawsuit arguing that facial recognition technology infringes the publicity rights of the person being scanned. I am actually surprised that, as of this writing, no one seems to have yet made this argument in court. Right of publicity law regulates the commercial exploitation of a person's identity, which is generally thought to include at least their physical appearance. The same commercial forces that guarantee the expansion of facial recognition will also provide plenty of evidence demonstrating the commercial value of the data. It will not take a scholar to connect the dots and argue that the people scanned should recoup a portion of any money made from their biometric data.

Whether this argument gains any traction is another matter. Biometric data is already widely used for entirely utilitarian (and especially security) purposes – witness, for example, the fingerprint scanner introduced in the iPhone 5S. Entire social networks and other user-generated content may come to rely on the ability to use facial recognition to identify specific individuals. As facial recognition capability becomes more democratized, allowing not only corporations to scan and store such data, the First Amendment may come to protect an individual's right to identify and annotate their knowledge of others in this manner. Allowing people to own intellectual property rights in that data might complicate matters too much for that technology to remain useful, to the detriment of society as a whole.

### THREE-DIMENSIONAL CAPTURE OF ENTIRE BODIES: SEX APPEAL AND THE RIGHT OF PUBLICITY

Traditional biometric indicators may not be the only way in which augmented technologies catalog and exploit individuals' physical attributes. Mass-market devices like Microsoft's Kinect are already designed to recognize entire bodies. A few years ago, artists in Spain set up a booth that used three Kinect cameras to scan individuals from head to toe. That data was relayed to a 3D printer in order to make a personalized figurine of the person right there on the street. Today, there are companies simultaneously using more than 60 sensors more precise than the Kinect to digitally render individuals in real time with amazing accuracy. Moreover, the year 2014 saw the introduction of the Kickstarter-funded Structure Sensor – an iPad accessory that allows the device's camera to capture three-dimensional imagery from its surroundings in real time – and Google's Project Tango, an experimental depth sensor that also renders ambient surroundings in 3D.

AR applications will take advantage of such capabilities in order to superimpose digital data on a person's entire body. Many of these will be benign; entire markets will develop for virtual clothing and accessories, for instance. Security professionals already scan entire bodies for contraband, and have made progress in identifying individuals based on their gait as well.[80]

---

78  Cohen v. Facebook, Inc., 798 F. Supp. 2d 1090 (ND Cal. 2011) and Fraley v. Facebook, Inc., 830 F. Supp. 2d 785 (ND Cal. 2011)
79  Eagle v. Morgan, No. 11-4303. (E.D. Penn. 2013)

80  "Gait biometrics shows promise," Homeland Security News Wire, September 8, 2011, available at http://www.homelandsecuritynewswire.com/gait-biometrics-shows-promise

Other applications, however, will go beyond merely analyzing images of bodies to storing and repurposing those images. In an age where sexting is an epidemic among teens and states like California are forced to outlaw the salacious repurposing of such content (i.e., "revenge porn"), it does not require much imagination to conceive of the unsavory uses to which 3D personal imaging technologies could be put. (I would be surprised if, by the time this book sees print, there have not already been instances of three-dimensional sexting.) To date, in courts across the country, one of the most frequent reasons for invoking the right of publicity has been to enjoin the prurient use of girls' and women's images, which are often recorded unwittingly. It is logical to expect the same laws to be applied when those images are collected and manipulated by new digital media.

How effective this right will be in these new augmented realms remains to be seen. The right of publicity has always existed in tension with the First Amendment's protection of free speech, and often finds itself pre-empted by the Copyright Act as well. Both of these more-established bodies of law are likely to keep publicity rights from expanding too broadly. But there is still quite a bit of conduct that falls within the gray area between these areas of law, where the boundaries have yet to be definitively drawn.

### "Profiting directly from their sex appeal"

In 2009, a 22-year-old college student calling herself Natalie Dylan sold her virginity to raise money for grad school. The bidding, conducted online for services to be rendered in Nevada, where prostitution is legal, went as high as $3.8 million. While her decision received a fair amount of criticism and moral approbation, she was also congratulated by the CEO of a Fortune 500 company for her "entrepreneurial gumption." Explaining her decision, Dylan wrote: "it became apparent to me that idealized virginity is just a tool to keep women in their place. But then I realized something else: if virginity is considered that valuable, what's to stop me from benefiting from that?… I took the ancient notion that a woman's virginity is priceless and used it as a vehicle for capitalism."[81]

"I might even be an early adopter of a future trend," Dylan predicted. "These days, more and more women my age are profiting directly from their sex appeal."[82]

She was right. The following year, the UK press profiled an 18-year-old Romanian girl who sold herself in exactly the same manner (but for far less money), citing Dylan as inspiration. Search engines reveal hordes of similar copycats. Still, Dylan concluded that "society isn't ready for

public auctions like mine – yet."[83] She's right about that, too. But are we moving in the direction of women commodifying themselves in order to "profit directly from their sex appeal," as Dylan suggests? There are reasons to believe we are – and that the right of publicity is providing the legal framework in which it can happen.

### Publicity rights as shields against prurient publications

Several courts have used the right of publicity to stop others from using plaintiff's image in a sexually suggestive manner. For example, Bret Michaels and Pamela Anderson won a lawsuit to block publication of their sex tape on this and other grounds.[84] More recently, Kim Kardashian argued that a sex doll bearing a striking resemblance to her violated her right of publicity.[85]

In 2004, Catherine Bosley, a local newscaster in Ohio, sued when a video of her participating in a wet t-shirt contest found its way online and went viral.[86] She won, but the reasoning the court used to reach that result raises some questions. For reasons I've discussed elsewhere in more depth, the logical implication of the court's holding is that, despite her pre-existing status as a "regional celebrity," Bosley's commercial value had nothing to do with her unique, personal "identity," as right of publicity case law has traditionally required. Rather, it came solely from the prurient value associated with her taking her top off. Several cases involving "Girls Gone Wild"-type situations have reached similar results. The implication of each ruling is that commercial value came from the plaintiff's body, not her identity.

In my home jurisdiction of Michigan, these questions were raised in the case of *Arnold v. Treadwell*.[87] There, a young aspiring model in Detroit posed for a photo shoot with local photographers, then sued them after some of those pictures (several of which were racy to begin with) ended up in a racy magazine, allegedly without her permission. She lost in the state trial court. But the Michigan Court of Appeals reversed, reasoning that the evidence could show "that there is value in associating an item of commerce with plaintiff's identity." The evidence supporting that finding? That "plaintiff has contracted to model clothing in a fashion show, to play an extra in a music video, and to work as an exotic dancer"[88] –all activities that involve exploiting her body, not her identity.

81   Natalie Dylan, Why I'm Selling My Virginity, The Daily Beast (January 23, 2009) http://www. thedailybeast.com/articles/2009/01/23/why-im-selling-my-virginity.html
82   Id.
83   Id.
84   Michaels v. Internet Entm't Grp., Inc., 5 F. Supp. 2d 823 (C.D. Cal. 1998)
85   Lisa Prince, Keeping Up With The Kardashians: Kim Kardashian Reacts To Sex Toy Doll, Reality TV Magazine (September 22, 2010)http://realitytvmagazine.sheknows.com/2010/09/22/keeping-up- with-the-kardashians-kim-kardashian-reacts-to-sex-toy-doll/
86   Bosley v. WildWett. Com, 310 F. Supp. 2d 914 (N.D. Ohio 2004)
87   Arnold v. Treadwell, No.2007-080617-CZ, 2009 WL 2136909 (Mich Ct. App. July 16, 2009) (unpublished opinion)
88   Id.

Only days after this ruling, a local Federal judge likewise refused to dismiss Arnold's parallel "false endorsement" claims under the Lanham Act.[89] The court's reasoning was slightly different than the state court's. The court only went so far as to note that Arnold had "a present intent to commercialize her identity." In other words, as long as Arnold had opened the door to commercially exploiting her own appearance, she would be allowed to make her case that her identity did, in fact, have commercial value. Nevertheless, there was still no discussion of the distinction between "likeness" and "identity."

Taken together, therefore, these cases demonstrate that the right of publicity (and related claims) can be an effective basis for attractive people to prevent others from publishing prurient images of them without permission. The means of achieving that result, however, is to think of those plaintiffs' bodies in purely commercial terms, and to legally equate their physical appearance with their identity as people.

### My body, my intellectual property

I am not necessarily suggesting that these cases were wrongly decided based on legal precedent, or even that their results are inevitably bad for society. To the contrary, judges have understandably latched onto publicity rights as one of the few effective mechanisms for putting an end to revenge porn and other exploitative content. It is an easier solution than copyright law, since copyrights vest by default in the person taking the picture, rather than the person depicted in the picture. Until we have better laws, or better judicial precedents, to rely on, the right of publicity may remain the best tool courts have for combatting revenge porn and other unquestionably destructive behavior.

But I do want to raise the question of whether, in the long run, using this doctrine in this way creates precedents that will ultimately make it easier for individuals – primarily young women – to exploit themselves in ways they will later come to regret. Admittedly, this is not an entirely new concept. Sex sells. That's a basic fact of human nature. Advertising a product by associating it with an attractive model is Marketing 101. Thousands of people have pursued modeling as a career, and there is nothing inherently questionable about that.

What rights should modeling get someone? Arnold was no supermodel – people who, in today's culture, are "celebrities" in every sense of the word. Rather, she had appeared in one, very local modeling show, as an extra in a music video, and as an exotic dancer. No one reading the magazine she sued over had any idea who she was; they only saw what she looked like. But the mere fact that she (and the plaintiffs in each of the other cas-

es discussed above) was attractive enough to appear in a magazine (or video) gave her legally enforceable rights to profit from the publication of her image.

With that principle established, the right of publicity increasingly forms the basis of a reliable business model for any reasonably attractive person looking to "profit directly from their sex appeal." And they don't even have to go as far as Natalie Dylan did in selling her actual body; images will do just fine. The right of publicity has been in the news a lot lately, thanks to pop stars like Kim Kardashian and Lindsey Lohan, actors like Sandra Bullock, Julia Roberts, and George Clooney, and the estates of Tupac Shakur, Elvis, and Marilyn Monroe. Especially in the face of high youth unemployment and a sagging economy, how long until more young people start putting two and two together, like Natalie Dylan or the protagonists of *The Full Monty* did?

Of course, whether and how much this happens depends on a lot more than intellectual property laws. It's a product of moral and ethical norms, societal attitudes, and much more. But having the legal mechanism in place to guarantee a profit may make it easier.

### VIRTUAL ASSISTANTS AS INFRINGEMENT

Apple has Siri. Microsoft has Cortana. Google has the yet-to-be-anthropomorphized Voice Search. The Oscar-nominated film *Her* featured Samantha, while Ender Wiggins (in the sequels to *Ender's Game*) had Jane. Vital to each iteration of the starship *Enterprise* was the Computer.

Futurists have long anticipated the day when humans could interact with computers using the same conversational speech we normally reserve for other people. In order to offer truly two-way interaction his type, however, the programs need to be able to respond in kind. In other words, they need to seem more human. The virtual assistants available as of this writing are beginning to approximate that experience. Siri has already reached its second generation, and some of its original creators are already at work on a next-generation competitor named "Viv" that is intended to be "blindingly smart," "infinitely flexible," "omnipresent," and "embedded in a plethora of Internet-connected everyday objects."[90]

But users and UX designers alike crave a more human-like interaction. AR will offer a unique avenue for achieving this goal by adding visual (and perhaps other sensory) elements to our digital companions. In the very near future, we will have available Siri-like assistants that we can actually see and communicate with faceto-face, via our digital eyewear. This sort of synthetic companion raises a variety of issues, some of which we will revisit in Chapters 7

89  Arnold v. Treadwell, 642 F. Supp. 2d 723 (E.D. Mich. 2009).

90  Steven Levy, "Siri's Inventors Are Building a Radical New AI That Does Anything You Ask," Wired, August 12, 2014, available at http://www.wired.com/2014/08/viv/

**Figure 13.** *Olivia holding "Eve."*

(re personal safety) and 13 (re pornography). Here, however, I want to suggest that those designing virtual people will inevitably mimic real people, and that this will potentially infringe the publicity rights of their muses.

The simple case in this hypothetical is the company that offers the likenesses of recognizable celebrities as "skins" for a virtual assistant. (This is already beginning to happen; in November 2013, the company behind the crowdsourced navigation app Waze announced a deal with Universal Pictures to allow the app to give directions in a celebrity's voice. The first such voice made available was that of comedian and actor Kevin Hart. [91]) That would amount to a commercial exploitation of an identity with defined monetary
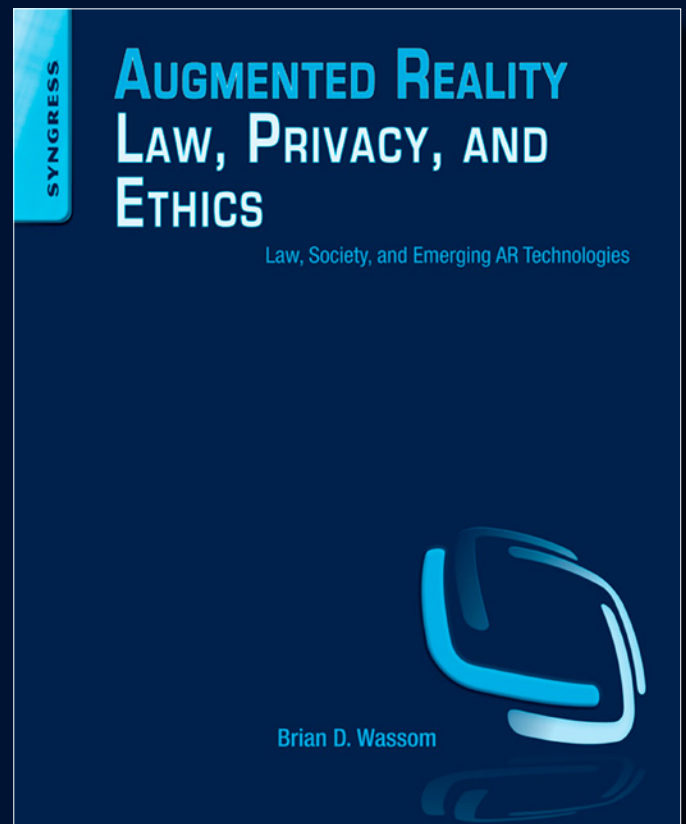
[91] "Waze debuts new feature where celebrities give you driving directions," VentureBeat, November 23, 2013, available at http://venturebeat.com/2013/11/23/waze-debuts-celebrity-voice-navigation-feature/

# Augmented Reality Law, Privacy, and Ethics
## Law, Society, and Emerging AR Technologies
*by Brian D. Wassom, Allison Bishop, Technical Editor*

*http://store.elsevier.com/*

value, a straightforward infringement. But what if the real-life inspiration behind the program is less recognizable, the similarity is less than exact, or the imitation is unauthorized?

These questions were explored in (of all places) *Drop Dead Diva*, a legal dramedy on the Lifetime Network. The June 2012 episode "Freak Show" begins with the premise of a woman named Olivia, who is bitter over the fact that her husband has been preoccupied with "Eve," the virtual assistant program that he created and is about to bring to market (Figure 13). Eve runs on a tablet computer and is clearly inspired by Apple's Siri. When Olivia fails to convince a judge that this amounts to infidelity, her lawyers then realize that Eve is programmed with a variety of biographical details–including her birth date, her hometown, her highest level of schooling – that all correspond to the Olivia's.

Olivia then uses these details to allege that Eve infringes her right of publicity. She cites the actual 1992 decision in *White v. Samsung Electronics America, Inc.,*[92] in which a Samsung commercial depicted a future *Wheel of Fortune* game show involving a faceless robot wearing a blond wig turned the letters. Vanna White prevailed on a claim that the robot misappropriated her likeness, even though the robot was an allusion to Vanna's occupation rather than her personal identity (Figure 14).

As it happens, *White v. Samsung* represents the outer boundaries of publicity rights law. In a vocal and well-reasoned dissent, Judge Kozinski lamented that "every famous person now has an exclusive right to anything that reminds the viewer of her." Both the Sixth and Tenth Circuits have explicitly rejected, and refused to follow, *White*'s logic. So its value as a basis for evaluating new technologies is questionable at best. Moreover, the facts of "Olivia v. Eve" would almost certainly fail to pass muster even under *White*'s version of the right. Even conceding that Eve could capture Olivia's "essence" even without mimicking her physical appearance, the overlap would have to be enough to at least suggest Olivia's identity to a rational consumer. Yet the only

92   White v. Samsung Elec. Am., Inc. 971 F. 2d 1395 (9th Cir. 1992)



**Figure 14.** *Vanna White and her alleged doppleganger*

"data points" we're told of that match up are what even Olivia's intrepid lawyers describes as "totally random stats." No one other than Olivia and her lawyers are likely to ever make the connection between Eve and Olivia. Nor does the episode give any reason to believe that Olivia's identity has any commercial value to speak of.

Nevertheless, digital avatars will be fertile grounds for right of publicity claims. These theories are likely to have greater resonance with respect to virtual assistants because of the commercial, utilitarian nature of the function that they perform. To be sure, similar issues will arise in more artistic contexts as well. In fact, we've already seen several analogous claims in recent years, involving "holograms" of such deceased celebrities as Tupac Shakur, Marilyn Monroe, Amy Winehouse, Freddie Mercury, and Michael Jackson. Publicity rights objections by Winehouse's heirs in 2014 put a stop to her hologram before it began. College athletes in both New Jersey and California won publicity rights lawsuits against video game manufacturers that incorporated the players' likenesses into football games. And several celebrities, including Bette Midler, Tom Waits, the Romantics, and Arnold Schwarzenegger, have asserted publicity rights claims against those with sound-alike voices. Nevertheless, these artistic expressions raise much more convincing First Amendment defenses than non-expressive uses of celebrity identities.

## ABOUT THE AUTHOR

*Brian D. Wassom litigates disputes and counsels clients from Fortune 50 companies to startups concerning copyright, trademark, publicity rights, privacy, and related intellectual property and advertising issues. He is a partner in the law firm of Honigman Miller Schwartz and Cohn LLP, and chairs the firm's Social, Mobile and Emerging Media Practice Group. Brian authors a popular blog on emerging media at Wassom. com that features the section Augmented Legality®, the first regular publication devoted to the law governing augmented reality. Brian presents regularly to industry groups, legal education seminars, and conferences across the country on intellectual property, digital media, and related topics.*

## TECHNICAL EDITOR BIOGRAPHY

*Allison Bishop is a highly experienced criminal reviewer with 10 years experience reviewing cases, criminal research, and criminal activity. Allison also works as a paralegal performing tasks such as briefing cases and reviewing case law and the working within the legal process. As an editor, Allison enjoys reviewing and editing works based on criminal justice, legal studies, security topics, and cybercrime. When Allison is not entrenched in studies, she loves to exercise, cook, and travel.*

# Dr.WEB®
since 1992

## The ERA of harmony and security
# New Dr.Web! version 10

- Brand new user interface
- Configuration as simple as ABC
- Honest protection against real threats

Comprehensive protection for Windows
Anti-virus for Mac OS X and Linux

Basic protection for Windows,
Mac OS X and Linux

**Dr.WEB®**
Security Space
for Windows, Mac OS X, Linux

2 PCs
1 year

**Dr.WEB®**
Anti-virus
for Windows, Mac OS X, Linux

2 PCs
1 year

Protection
for any and
all devices*

Home
and office

+150  New
purchase
and renewal

\* PC, Mac and mobile devices running
OS supported by Dr.Web.

# Protection for mobile
# devices — for free!

© Doctor Web Ltd.
2003 — 2015

Doctor Web is the Russian developer of Dr.Web anti-virus software. Dr.Web anti-virus software has been developed since 1992. Doctor Web is one of the few anti-virus vendors in the world to have its own technologies to detect and cure malware. Dr.Web anti-virus software allows IT environments to effectively withstand any threats, even those not yet known.

# "IN SOME CASES
# nipper studio
## HAS VIRTUALLY
# REMOVED
## the NEED FOR a
# MANUAL AUDIT"
## CISCO SYSTEMS INC.

Titania's award winning Nipper Studio configuration auditing tool is helping security consultants and end-user organisations worldwide improve their network security. Its reports are more detailed than those typically produced by scanners, enabling you to maintain a higher level of vulnerability analysis in the intervals between penetration tests.

Now used in over 65 countries, Nipper Studio provides a thorough, fast & cost effective way to securely audit over 100 different types of network device. The NSA, FBI, DoD & U.S. Treasury already use it, so why not try it for free at www.titania.com

**www.titania.com**

# Take your Android development skills to the next level!

Whether you're an enterprise developer, work for a commercial software company, or are driving your own startup, if you want to build Android apps, you need to attend AnDevCon!

# AnDevCon
## The Android Developer Conference
## July 29-31, 2015
## Sheraton Boston

**Right after Google IO!**

- **Choose from more than 75 classes and in-depth tutorials**
- **Meet Google and Google Development Experts**
- **Network with speakers and other Android developers**
- **Check out more than 50 third-party vendors**
- **Women in Android Luncheon**
- **Panels and keynotes**
- **Receptions, ice cream, prizes and more**
  (plus lots of coffee!)

## Android is everywhere!
## But AnDevCon is where you should be!

### Earn your Certificate!
Enhance your skills and professional qualifications as an Android expert with over 23 hours of hardcore Android training!

AnDevCon
Certificate of Completion
John Doe
AnDevCon 2015
July 29-31, 2015
Boston, MA

"There are awesome speakers that are willing to share their knowledge and advice with you."
—Kelvin De Moya, Sr. Software Developer, Intellisys

"Definitely recommend this to anyone who is interested in learning Android, even those who have worked in Android for a while can still learn a lot."
—Margaret Maynard-Reid, Android Developer, Dyne, Inc.

# Register Early and Save at www.AnDevCon.com